Załącznik nr 1
Szczegółowy opis przedmiotu zamówienia

Modyfikacja z 19.02.2025r.

Strzyżów, Listopad 2024

Spis treści

1. E-usługi

Zamawiający wskazuje, że głównym celem zamówienia jest uruchomienie w Gminie nowych oraz modernizacja istniejących e-usług zgodnie z poniższym opisem.
Uruchomienie nowych i zmodernizowanych e-usług jest warunkiem dokonania odbioru końcowego całego zamówienia.
Zamawiający w ramach zamówienia wymaga realizacji następujących e-usług:

Lp.	Nazwa usługi	Rodzaj usługi	Poziom dojrzałości w projekcie	Systemy informatyczne\ i aplikacje, za pomocą których usługi te będą świadczone
1	**e-Należności / e-Płatności**	**A2C**	**5**	**eBOM, Aplikacja mobilna, oprogramowanie dziedzinowe, obieg dokumentów**

W ramach systemu eBOM każdy użytkownik będzie posiadał własne konto klienta.
Autoryzacja petentów będzie oparta o Krajowy Węzeł Identyfikacji Elektronicznej, w tym zakresie konieczna będzie dostawa certyfikatów wymaganych przez administratora tej platformy (Departament Tożsamości Cyfrowej, Centralny Ośrodek Informatyki). Planowana jest także integracja z elektronicznym obiegiem dokumentów celem udostępnienia akt sprawy zainteresowanym stronom postępowania. Portal w zakresie obsługi petentów uwierzytelnionych udostępniał im będzie usługi związane z realizowanie **płatności za wszelkie zobowiązania rejestrowane w systemie dziedzinowym urzędu** w szczególności:

a) płatności z tytułu podatków (rolny, leśny, od nieruchomości, podatek od środków transportowych) dla osób fizycznych i prawnych;
b) płatności z tytułu pozostałych opłat dla osób fizycznych i prawnych;
c) płatności z tytułu opłat cywilno-prawnych dla osób fizycznych i prawnych;
d) płatności z tytułu zezwoleń na sprzedaż napojów alkoholowych;
e) pozostałe zobowiązania wynikające z działalności urzędu;

Efektem uruchomienia usługi e-Należności będzie uruchomienie następujących spraw:

1. Płatność za Podatek od środków transportowych – po zalogowaniu się Podatnik będzie miał możliwość podglądu należności i dokonania płatności za pomocą eBOM. Zapłata należności kartą kredytową lub przelewem (integracja z operatorami płatności) – pozwala na łatwe i szybkie pokrycie należności poprzez kanał elektroniczny.
2. Płatność za Podatek od nieruchomości – po zalogowaniu się Podatnik będzie miał możliwość podglądu należności i dokonania płatności za pomocą eBOM. Zapłata należności kartą kredytową lub przelewem (integracja z operatorami płatności) – pozwala na łatwe i szybkie pokrycie należności poprzez kanał elektroniczny.
3. Płatność za Podatek od gruntów rolnych – po zalogowaniu się Podatnik będzie miał możliwość podglądu należności i dokonania płatności za pomocą eBOM. Zapłata należności kartą kredytową lub przelewem (integracja z operatorami płatności) – pozwala na łatwe i szybkie pokrycie należności poprzez kanał elektroniczny.
4. Płatność za Podatek od gruntów zalesionych (lasy) – po zalogowaniu się Podatnik będzie miał możliwość podglądu należności i dokonania płatności za pomocą eBOM. Zapłata należności kartą kredytową lub przelewem (integracja z operatorami płatności) – pozwala na łatwe i szybkie pokrycie należności poprzez kanał elektroniczny.
5. Płatność za Dzierżawę gruntu – po zalogowaniu się Podatnik będzie miał możliwość podglądu należności i dokonania płatności za pomocą eBOM. Zapłata należności kartą kredytową lub przelewem (integracja z operatorami płatności) – pozwala na łatwe i szybkie pokrycie należności poprzez kanał elektroniczny.
6. Płatność za Przekształcenie wieczystego użytkowania w prawo własności – po zalogowaniu się Podatnik będzie miał możliwość podglądu należności i dokonania płatności za pomocą eBOM. Zapłata należności kartą kredytową lub przelewem (integracja z operatorami płatności) – pozwala na łatwe i szybkie pokrycie należności poprzez kanał elektroniczny.
7. Płatność za Gospodarowanie Odpadami Komunalnymi (wywóz śmieci) – po zalogowaniu się Podatnik będzie miał możliwość podglądu należności i dokonania płatności za pomocą eBOM. Zapłata należności kartą kredytową lub przelewem (integracja z operatorami płatności) – pozwala na łatwe i szybkie pokrycie należności poprzez kanał elektroniczny.
8. Płatność za Zajęcie pasa drogowego – po zalogowaniu się Podatnik będzie miał możliwość podglądu należności i dokonania płatności za pomocą eBOM. Zapłata należności kartą kredytową lub przelewem (integracja z operatorami płatności) – pozwala na łatwe i szybkie pokrycie należności poprzez kanał elektroniczny.

W ramach realizacji płatności portal udostępni petentom informacje o źródle ich pochodzenia oraz sposobie naliczania z możliwością pobrania dokumentów ustalających dane zobowiązania (decyzja, deklaracja lub informacja podatkowa, nota obciążeniowa, upomnienie lub wezwanie do zapłaty, fakturą itp.). System zapewni pełna personalizację wpłat (poziom 5 e-usług), obejmujący automatyczne wypełnienie danych płatnika, tytułu zobowiązania, kwoty należnej wpłaty, rachunku bankowego na który należy dokonać wpłaty, wysokości ewentualnych odsetek od nieterminowej wpłaty oraz kosztów związanych z jej egzekucją. Rozwiązanie zapewni integracje z systemem płatniczym obsługującym płatności bezpośrednio z konta zobowiązanego, możliwość zapłaty kartą płatniczą oraz systemem płatności mobilnych BLIK. Portal eBOM w ramach swojej funkcjonalności udostępni petentom usługę pobierania dokumentów bezpośrednio z teczek spraw: e-dostęp do teczki sprawy.

2	**e-Woda**	**A2C**	**5**	**eBOM, Aplikacja mobilna, oprogramowanie dziedzinowe, obieg dokumentów, e-woda**

Usługa będzie świadczona w ramach systemu eWoda, w połączeniu z systemem eBOM. Każdy użytkownik posiadający podpisaną umowę na dostawę wody/odprowadzanie ścieków będzie posiadał własne konto klienta. Logowanie do konta będzie odbywać się z wykorzystaniem Krajowego Węzła Identyfikacji Elektronicznej.
Głównym zadaniem Platformy w systemie eWoda będzie generowanie danych o zużyciu wody odbiorców, na podstawie których będzie możliwe świadczenie poprzez system eBOK e-usługi na 5 poziomie dojrzałości w zakresie rzeczywistego rozliczenie odbiorcy w cyklu miesięcznym. Wystawione dokumenty będą możliwe do przeglądania, pobierania. W ramach systemu możliwe będzie również dokonanie płatności za należności z tytułu wody i ścieków. W ramach systemu zostaną dodatkowo udostępnione podpisane umowy i wnioski dotyczące ich zawarcia oraz zmiany. Dokumenty te będą możliwe do przesłania za pośrednictwem systemu obiegu dokumentów do odpowiednich jednostek. Po podpisaniu będą udostępniane na koncie klienta.

Dane zebrane w systemie eWoda posłużą zgodnie z Dyrektywą 2020/2184 do:
- rozliczenia Gminy z odbiorcą wg rzeczywistych zużyć,
- informowania odbiorcy o jego „bilingu" zużycia oraz ewentualnych wyciekach.
- bilansowania wody w tym samym momencie dla danego obszaru (rejestracja i określenie wielkości wycieku – strat wody)

Efektem uruchomienia usługi e-Woda będzie uruchomienie następujących spraw:

1. Sprawdzenie zobowiązania za zużycie wody i ścieków wraz z możliwością dokonania płatności elektronicznej –
   Po zalogowaniu się Usługobiorca będzie miał możliwość podglądu należności i dokonania płatności za pomocą Portalu. Zapłata należności kartą kredytową, przelewem (integracja z operatorami płatności). Po wdrożeniu sprawy i udostępnieniu jej na Portalu, Usługobiorca, czyli obywatel będzie posiadał możliwość zautomatyzowanego, pełnego załatwienia sprawy przez Internet, bez konieczności wizyty w Przedsiębiorstwie, przez 7 dni w tygodniu, 24 godziny na dobę, bez względu na miejsce przebywania.
2. Wniosek o zawarcie umowy na dostawę wody, odbiór ścieków - 4 poziom dojrzałości, oddziaływanie A2C,
   Po zalogowaniu się Usługobiorca będzie miał możliwość złożenia wniosku o zawarcie umowy na dostawę wody, odbiór ścieków. Po wdrożeniu e-Usługi i udostępnieniu jej na Portalu, Usługobiorca, czyli obywatel będzie posiadał możliwość zautomatyzowanego, pełnego załatwienia sprawy przez Internet, bez konieczności wizyty w Przedsiębiorstwie, przez 7 dni w tygodniu, 24 godziny na dobę, bez względu na miejsce przebywania.
3. Wniosek o zawarcie umowy na wywóz nieczystości płynnych - 4 poziom dojrzałości, oddziaływanie A2C,
   Po zalogowaniu się Usługobiorca będzie miał możliwość złożenia wniosku o zawarcie umowy na dostawę wody, odbiór ścieków. Po wdrożeniu e-Usługi i udostępnieniu jej na Portalu, Usługobiorca, czyli obywatel będzie posiadał możliwość zautomatyzowanego, pełnego załatwienia sprawy przez Internet, bez konieczności wizyty w Przedsiębiorstwie, przez 7 dni w tygodniu, 24 godziny na dobę, bez względu na miejsce przebywania.
4. Wniosek o wydanie warunków na montaż podlicznika - 4 poziom dojrzałości, oddziaływanie A2C,
   Po zalogowaniu się Usługobiorca będzie miał możliwość złożenia wniosku o wydanie warunków na montaż podlicznika. Po wdrożeniu e-Usługi i udostępnieniu jej na Portalu, Usługobiorca, czyli obywatel będzie posiadał możliwość zautomatyzowanego, pełnego załatwienia sprawy przez Internet, bez konieczności wizyty w Przedsiębiorstwie, przez 7 dni w tygodniu, 24 godziny na dobę, bez względu na miejsce przebywania.
5. Wniosek o zmianę danych na umowie/ fakturze - 4 poziom dojrzałości, oddziaływanie A2C,
   Po zalogowaniu się Usługobiorca będzie miał możliwość zmiany danych na umowie i danych do faktury. Po wdrożeniu e-Usługi i udostępnieniu jej na Portalu, Usługobiorca, czyli obywatel będzie posiadał możliwość zautomatyzowanego, pełnego załatwienia sprawy przez Internet, bez konieczności wizyty w Przedsiębiorstwie, przez 7 dni w tygodniu, 24 godziny na dobę, bez względu na miejsce przebywania.
6. Zlecenie zamontowania wodomierza na wodę bezpowrotnie zużytą - 4 poziom dojrzałości, oddziaływanie A2C,
   Po zalogowaniu się Usługobiorca będzie miał możliwość złożenia zlecenia zamontowania wodomierza na wodę bezpowrotnie zużytą. Po wdrożeniu e-Usługi i udostępnieniu jej na Portalu, Usługobiorca, czyli obywatel będzie

	posiadał możliwość zautomatyzowanego, pełnego załatwienia sprawy przez Internet, bez konieczności wizyty w Przedsiębiorstwie, przez 7 dni w tygodniu, 24 godziny na dobę, bez względu na miejsce przebywania			
3	e-Rada	A2C	4	eBOM, Aplikacja mobilna, obieg dokumentów, e-Rada
Usługa pozwalająca zainteresowanej osobie poprzez stronę internetową na uczestnictwo on-line w sesji rady gminy (z możliwością pełnego uczestnictwa, interakcja dwustronna, zadawanie pytań, dyskusja) oraz na dostęp do formularzy elektronicznych modułu interpelacje i zapytania, materiałów archiwalnych nagrań–sesji rady. Usługa wspomagający prace rady gminy oraz jej kontakt z mieszkańcami gminy Projekt zakłada modernizację usługi eRada dotyczącej transmisji obrad Rady oraz uczestnictwa w niej mieszkańców. Obecnie system eRady nie pozwala na uczestnictwo w spotkania przez mieszkańców. Realizowany jest jedynie streaming posiedzeń oraz publikacja informacji z nich. Docelowo nowa e-usługa pozwoli mieszkańcom na branie udziału w posiedzeniach rady i zabieranie na nich głosu, a także zadawanie pytań i uzyskiwanie odpowiedzi. Ponadto system eRady zostanie połączony z systemem obiegu i udostępniania dokumentów dla radnych, co usprawni ich dystrybucję. System pozwoli zatem na włączenie mieszkańców w życie gminy i zwiększenie ich udziału w społeczeństwie obywatelskim. Obsługa e-usług w zakresie E-RADA będzie realizowana według poniższych założeń: a) Określenie terminów sesji rady – harmonogramu z wykorzystaniem dedykowanego oprogramowania. b) Przekazanie informacji - link do wirtualnej platformy spotkania, transmisje on-line – strona WWW. c) Przygotowanie materiałów na sesję – dane zarządzane przez biuro rady. Radny otrzymuje informacje, że materiały są dostępne. d) Publikacja materiałów - radny pobiera materiały ze strony WWW. e) Uruchomienie i zarzadzanie sesją według wcześniej przygotowanego harmonogramu. f) Użytkownik ma dostęp do obrad rady poprzez system transmisji on-line. g) Dostęp do strumienia video poprzez stronę eBOK – brak konieczność uwierzytelnienia. h) Zarzadzanie sesją: tworzenie sprawozdań, obsługa głosowań itp. Archiwizacja spotkania (nagranie na zasób dyskowy). Publikacja danych ze spotkania – sieciowe repozytorium danych.				
4	e-Edukacja	A2C	4	eBOM, Aplikacja mobilna, oprogramowanie dziedzinowe, obieg dokumentów, e-dziennik
Usługa elektroniczna pozwalająca opiekunowi prawnemu dziecka na dostęp do zasobów dziennika elektronicznego poprzez zestaw formularzy, raportów oraz analiz. Pozwala na śledzenie postępów w nauce oraz kontakt dwustronny z placówka oświatową, a także na zatwierdzanie danych transakcyjnych np. nieobecności dziecka w szkole, zgód na wyjazdy, wyjścia, itp. Obsługa e-usług w zakresie „e-edukacja" będzie realizowana według poniższych założeń: a) Nauczyciel loguje się do systemu b) Wprowadza, modyfikuje dane w systemie poprzez formularze elektroniczne np.: oceny, tematy lekcji itp. c) Oprogramowanie dziedzinowe zapisuje dane w rejestrach, analizuje zakres przetwarzania oraz wymagane składniki (moduły) systemu dziedzinowego. d) Oprogramowanie dziedzinowe przetwarza dane za pomocą dostępnych funkcji. e) Następuje transakcja na wprowadzanych danych. Dane gotowe do przekazania dla opiekuna. f) Opiekun dziecka loguje się na stronie WWW g) Wyszukuje interesujące go dane między innymi poprzez formularz elektroniczny. h) Dane są przetwarzane on-line i wyświetlane. i) opiekun ma możliwość dokonania transakcji np. usprawiedliwienia nieobecności dziecka w szkole, zgłoszenia nieobecności, wydania zgody na określoną aktywność, itp.				
5	e-Geodezja	A2C	5	eBOM, Aplikacja mobilna, oprogramowanie dziedzinowe, obieg dokumentów, Oprogramowanie GIS

Sprawy do załatwienia z zakresu systemu GIS będą udostępnione w ramach jednej platformy eBOM oraz w aplikacji mobilnej, w usłudze e-Geodezja. Zakłada się osiągnięcie 5 poziomu dojrzałości tj. możliwości zapłaty za usługę. Wszystkie usługi będą dostępne po zalogowaniu na własne konto klienta. System logowania zostanie oparty o węzeł krajowy.
W ramach usługi e-geodezja zaplanowano realizację następujących spraw ważnych dla mieszkańca, np.:
1. Wypisy, wyrysy i zaświadczenia z MPZP/SUiKZP
2. Procedura planistyczna dla MPZP/SUiKZP
3. Gminna Ewidencja Zabytków

W każdym wypadku proces świadczenia usługi obejmie procedowanie wniosku, wydanie decyzji i wystawienie druku opłaty oraz umożliwienie jej uiszczenia w ramach systemu. Pozwoli to na skrócenie czasu realizacji usługi, usprawnienie jej przebiegu oraz uzyskanie wysokiej efektywności jej świadczenia.

2. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

- całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
- całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

3. Wymagania gwarancyjne.

Sprzęt

- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
- Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
- Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;
- wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

Oprogramowanie

- oprogramowanie powinno posiadać min. 36-miesięczną gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);
- gwarancja nie obejmuje kosztów bieżącego utrzymania (opieka serwisowa, upgrade systemów, wersji, prawa do aktualizacji) wdrożonego oprogramowania po okresie realizacji projektu.

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

4. Miejsce instalacji sprzętu i oprogramowania/systemu.

- Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu, w budynkach urzędu lub budynkach jednostek podległych, w miejscach wskazanych przez Zamawiającego.

5. Zestawienie zakresu dostaw i usług.

5.1. Zestawienie zakresu dostaw i usług – część 1

Lp.	Nazwa środka trwałego lub wartości niematerialnych i prawnych itp.	Wymagana minimalna długość gwarancji (m-ce)	Typ/Rodzaj gwarancji	Ilość	Jednostka miary
1.	Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa	36	Producenta/Wykonawcy	1	lic.
2.	Oprogramowanie do zarzadzania infrastrukturą IT	36	Producenta/Wykonawcy	1	lic.
3.	Oprogramowanie do wirtualizacji	36	Producenta/Wykonawcy	1	lic.
4.	Oprogramowanie do backupu	36	Producenta/Wykonawcy	1	lic.
5.	Macierz dyskowa	36	Producenta/Wykonawcy	1	szt.
6.	Klaster firewall	36	Producenta/Wykonawcy	1	szt.
7.	Centralny system logów	36	Producenta/Wykonawcy	1	szt.
8.	Zestaw komputerowy z oprogramowaniem	36	Producenta/Wykonawcy	35	szt.
9.	Laptop z oprogramowaniem	36	Producenta/Wykonawcy	5	szt.
10.	UPS	36	Producenta/Wykonawcy	1	szt.
11.	Agregat	36	Producenta/Wykonawcy	1	szt.
12.	Instalacja i konfiguracja (Platforma sprzętowa)	36	Wykonawcy	100	Rbh
13.	Szkolenia TiK typ I	Nd	Nd	120	rbh

5.2. Zestawienie zakresu dostaw i usług – część 2

Lp.	Nazwa środka trwałego lub wartości niematerialnych i prawnych itp.	Wymagana minimalna długość gwarancji (m-ce)	Typ/Rodzaj gwarancji	Ilość	Jednostka miary
1.	eBOM - elektroniczne Biuro Obsługi Mieszkańca	36	Producenta/Wykonawcy	1	lic.
2.	Oprogramowanie dziedzinowe	36	Producenta/Wykonawcy	1	lic.
3.	Planowanie budżetu	36	Producenta/Wykonawcy	1	lic.
4.	System GIS	36	Producenta/Wykonawcy	1	lic.
5.	e-edukacja	36	Producenta/Wykonawcy	1	lic.
6.	Obieg dokumentów	36	Producenta/Wykonawcy	50	lic.
7.	Monitoring środowiska	36	Producenta/Wykonawcy	1	zestaw
8.	PSZOK	36	Producenta/Wykonawcy	1	lic.
9.	eRada	36	Producenta/Wykonawcy	1	lic.
10.	e-Rada sprzęt komputerowy	36	Producenta/Wykonawcy	1	kpl.
11.	Wodomierze z nakładka radiową	36	Producenta/Wykonawcy	1397	szt.
12.	System eWoda	36	Producenta/Wykonawcy	1	lic.
13.	Integracja (Platforma e-usług publicznych)	36	Wykonawcy	400	rbh
14.	Instalacja i konfiguracja (Platforma e-usług publicznych)	36	Wykonawcy	200	rbh
15.	Digitalizacja zasobów	Nd	Nd	100	rbh

16.	Szkolenia TiK Typ II	Nd	Nd	168	rbh

6. Szczegółowy opis pozycji – część 1.

6.1. Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa – licencja szt. 1 – wymagania minimalne

System przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.

1. System musi umożliwić odbieranie logów z urządzeń sieciowych oraz wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
2. System musi zapewnić agentów XDR na stacje końcowe umożliwiających im pobieranie pełnych danych telemetrycznych hostów których chronią i przesłanie tych danych do systemu centralnego w celu dalszej korelacji i analizy behawioralnej. W przypadku wykrycia zagrożenia agenci muszą umożliwiać automatyczną i dostosowaną do kontekstu reakcje, m.in. na blokowanie bądź izolację sieciową złośliwego oprogramowania.
   - 2.1. Agent musi posiadać możliwość dodawania i usuwania reguł wbudowanego firewalla obejmując m.in. blokowanie i odblokowywanie poszczególnych procesów bądź reguł dotyczących ruchu sieciowego stanowiące reakcję na wykryte zagrożenie.
   - 2.2. Agent musi pobierać oraz aktualizować na bieżąco listę zainstalowanego oprogramowania.
   - 2.3. System w przypadku wykrycia techniki ataku ukierunkowanego na podatną aplikację w celu zablokowania ataku musi umożliwiać zatrzymanie procesu aplikacji oraz zapewnić dostęp do danych dowodowych obejmujących nazwę chronionego systemu, system operacyjny, tożsamość użytkownika, nazwę procesu, dokładną komendę uruchamiającą złośliwy proces wraz parametrami i znacznik czasowy.
   - 2.4. System musi obsługiwać scenariusz uwzględniający ocenę prawdopodobieństwa materializacji się wykrytego zagrożenia, gdzie w przypadku gdy wyliczone przez system prawdopodobieństwo ataku jest wysokie proces zostanie zablokowany, natomiast w pozostałych przypadkach gdy jest ono średnie bądź niskie zostanie on zamrożony z możliwością ponownego wznowienia przez operatora.
   - 2.5. System musi posiadać możliwość dostosowania reakcji na zagrożenie w zależności od rodzaju zasobu który chroni, przykładowo jeżeli zagrożenie dotyczyć będzie procesu na stacji roboczej proces zostanie automatycznie zablokowany jednakże w przypadku gdy to samo zagrożenie dotyczyć będzie serwera świadczącego usługi w sieci publicznej proces pozostanie uruchomiony z jednoczesną blokadą publicznego ruchu przychodzącego.
3. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;
4. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
5. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
6. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
7. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.
8. 9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.
9. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o

nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.

10. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku gdy będzie to konieczne przywrócić jedną z poprzednich wersji.
11. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg" znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.
12. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni w której te logi są przesyłane. Przykładowo jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.
13. 14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.
14. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.
15. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.
16. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.
17. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe.
18. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
19. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.
20. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.
21. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.
22. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.
23. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa

oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie" na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.

24. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.
25. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.
26. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.
27. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.
28. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:
    a. nowe zasoby wykryte w sieci,
    b. typy wykrytych zasobów (np.: serwer lub stacja robocza),
    c. zastosowane na nich zabezpieczenia,
    d. usługi z którymi się komunikują,
    e. nowe usługi wykryte na zasobie
    f. komunikację do usług wykrytych na zasobie.
29. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
30. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.
31. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi której ta komunikacja dotyczy.
32. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:
    a. fqdn,
    b. e-mail,
    c. nazwa pliku,
    d. ścieżka do pliku,
    e. hash,
    f. adres IP,
    g. klucz rejestru,
    h. cmd.
33. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/).
34. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).
35. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs", „Malicious domain" czy „Tor Exit Nodes").
36. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login,

e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.

37. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
38. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).
39. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
40. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.
41. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.
42. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:
    a. id techniki,
    b. taktykę,
    c. platformy których dotyczy,
    d. potencjalne źródła,
    e. opis zagrożenia,
    f. mityzację,
    g. sposób detekcji,
    h. referencje.
43. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
44. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).
45. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:
    a. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,
    b. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,
    c. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,
    d. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.
46. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).
47. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.
48. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).

49. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
50. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.
51. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:
    a. sparsowane pola oraz ich wartości,
    b. listy referencyjne,
    c. atrybuty użytkowników z Active Directory,
    d. atrybuty komputerów z Active Directory,
    e. bazę wskaźników kompromitacji (IOC),
    f. informacje z elektronicznej dokumentacji,
    g. anomalie w zachowaniu użytkowników (UBA),
    h. anomalie w zachowaniu zasobów (EBA),
    i. podatności na zasobach,
    j. wyniki analizy konfiguracji,
    k. techniki MITRE ATT&CK®,
52. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:
    a. wykrycie dowolnej treści w logach,
    b. wykrycie zmiany jednego z kilku pól,
    c. wykrycie zaniku wiadomości,
    d. wykrycie nowej wartości pola w zadanym okresie czasu,
    e. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
    f. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,
    g. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,
    h. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
    i. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,
    j. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,
    k. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
    l. wykrycie ilości uruchomionych procesów w zadanym okresie czasu,
    m. wykrycie skanowania portów.
53. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:
    a. wykrycie wystąpienia wartości pola na wybranej liście,
    b. wykrycie niewystępowania wartości pola na wybranej liście,
    c. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku z którego został uruchomiony),
    d. wykrycie niewystąpienia pary wartości na wybranej liście
    e. (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).
54. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:
    a. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
    b. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,
    c. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).
    d. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),
    e. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.
55. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:

a. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,
b. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,
c. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.

56. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:
    a. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;
    b. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;
    c. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;
57. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:
    a. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,
    b. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,
    c. wykrycie nieautoryzowanej usługi na serwerze,
    d. wykrycie nieautoryzowanego połączenia do usługi na serwerze,
    e. wykrycie nieautoryzowanego połączenia z serwera usług,
    f. wykrycie nieautoryzowanego połączenia do sieci Internet.
58. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:
    a. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
    b. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,
    c. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
    d. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.
59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:
    a. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
    b. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
    c. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
    d. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.
60. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:
    a. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
    b. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
    c. wykrycie zdarzeń o wysokim „severity" na zasobach posiadającego krytyczne podatności,
    d. wykrycie zdarzeń o wysokim „severity" do zasobów posiadających krytyczne podatności.
61. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:
    a. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków,
    b. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
62. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:
    a. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
    b. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
    c. wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.
63. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:
    a. wykrycie anomalii na koncie uprzywilejowanym użytkownika,
    b. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście

referencyjnej,
   c. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
   d. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,
   e. wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
64. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:
   a. sparsowane pola oraz ich wartości,
   b. atrybuty użytkowników z Active Directory,
   c. atrybuty komputerów z Active Directory,
   d. informacje z elektronicznej dokumentacji.
65. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:
   a. adresie IP,
   b. koncie domenowym użytkownika,
   c. strefie bezpieczeństwa,
   d. zakresie adresów IP.
66. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop" umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.
67. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.
68. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.
   a. wszystkie skorelowane zdarzenia,
   b. korespondencja pocztowa,
   c. załączniki z próbkami lub dowodami,
   d. wskaźniki kompromitacji (IoC),
   e. informacje pozyskane z innych systemów.
69. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.
70. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa.
71. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:
   a. identyfikację celu i źródła zagrożenia,
   b. nazwę oraz adres IP źródła zagrożenia,
   c. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
   d. lokalizację z które pochodzi zagrożenie np.: Internet,

e. strefę bezpieczeństwa z której pochodzi zagrożenie,
f. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
g. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
h. nazwę oraz adres IP celu zagrożenia,
i. zabezpieczenia lokalne chroniące cel zagrożenia,
j. strefę bezpieczeństwa w której znajduje się cel zagrożenia.

72. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).
73. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.
74. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie:
    a. nazwy zasobu,
    b. rodzaju zasobu,
    c. ważności zasobu dla organizacji,
    d. rodzaj przetwarzanych informacji,
    e. usług, które ten zasób świadczy,
    f. lokalizację użytkowników, którzy z niego korzystają,
    g. usługi z których zasób korzysta.
75. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.
76. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:
    a. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
    b. segregacja – segregacja i kwalifikacja zdarzeń,
    c. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
    d. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,
    e. zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie.
77. System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”.
78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.
79. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie

każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych.

80. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.
81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.
82. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.
83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.
84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:
    a. podgląd aktywności zagrożonego zasobu na linii czasu,
    b. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,
    c. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,
    d. podgląd reguły korelacyjnej, która wygenerowała zdarzenie,
    e. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,
    f. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,
    g. gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o:
        - listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
        - listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
    h. gotowe i proste w użyciu filtry rozszerzajcie analizę logów o:
        - listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
        - listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.
85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
    a. warunki powiadomień,
        - zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
        - zdarzeń o przekroczonych czasach SLA o definiowalny okres,
        - zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
        - zdarzeń, których priorytet osiągnął określoną wartość,
        - zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
        - zdarzeń na których doszło do naruszenia bezpieczeństwa,
        - zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
        - zdarzeń realizujących zdefiniowaną usługę,
        - zdarzeń przetwarzających sklasyfikowane informację,
        - zdarzeń przetwarzanych na krytycznych zasobach,
    b. odbiorców powiadomień, w tym:
        - operatora, któremu zostało przydzielone zdarzenie,
        - właściciela zasobu na którym wystąpiło zdarzenie,
        - zespół obsługi, który odpowiada za obsługę zdarzeń,
        - właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie,
        - podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.
    c. kanały powiadomień, m.in. e-mail, sms, komunikator,
    d. zastosowanie mechanizmów grupowania:

- grupowanie wielu powiadomień w jednej wiadomości,
- ograniczenie liczby wierszy powiadomienia do określonej wartości.

86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:
    a. utworzenia nowego zdarzenia z określonym priorytetem,
    b. utworzenia nowego zdarzenia na zasobie krytycznym,
    c. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
    d. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
    e. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
    f. modyfikacji przydzielonego operatorowi zdarzania przez innego operatora,
    g. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora,
    h. przejęcia przydzielonego operatorowi zdarzania przez innego operatora.
87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:
    a. wybór raportu, który ma zostać wysłany,
    b. zdefiniowanie jego tytułu,
    c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
    d. możliwość ograniczenia cyklu do dni powszednich,
    e. określenie daty przesłania pierwszego raportu,
    f. możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
        - zdefiniowanej daty końcowej,
        - określnej liczby raportów,
    g. określenie odbiorców raportu.
88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).
89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:
    a. strefę bezpieczeństwa w której została wykryta podatność,
    b. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
    c. rodzaj zasobu którego dotyczy ta podatność,
    d. ważność tego zasobu dla organizacji,
    e. przetwarzane na tym zasobie informacje, np.: dane osobowe,
    f. usługi realizowane przez ten zasób, np.: DNS,
    g. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,
    h. poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
    i. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.
90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.
91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:
    a. wyliczonym priorytecie podatności,
    b. aktualnym statusie obsługi,
    c. ważności zasobu na którym została wykryta,
    d. adresie IP tego systemu,
    e. parametrów SLA związanych z tym statusem,
    f. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
    g. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV) = „Network”.

92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:
    a. przekroczenia czasu reakcji o określony czas np.: o godzinę,
    b. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
    c. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
    d. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,
    e. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,
    f. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
    g. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
    h. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
    i. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
    j. przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
    k. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,
93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
    a. warunki powiadomień,
        - podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
        - podatności o przekroczonych czasach SLA o definiowalny okres,
        - podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
        - podatności, których priorytet osiągnął określoną wartość,
        - zdarzeń realizujących zdefiniowaną usługę,
        - zdarzeń przetwarzających sklasyfikowane informację,
        - zdarzeń przetwarzanych na krytycznych zasobach,
    b. odbiorców powiadomień, w tym:
        - operatora, któremu została przydzielona podatność,
        - właściciela zasobu na którym wystąpiła podatność,
        - zespół obsługi, który odpowiada za obsługę podatności,
        - właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność,
        - podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.
    c. kanały powiadomień, m.in. e-mail, sms, komunikator,
    d. zastosowanie mechanizmów grupowania:
        - grupowanie wielu powiadomień w jednej wiadomości,
        - ograniczenie liczby wierszy powiadomienia do określonej wartości.
94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:
    a. przydzielenia nowej podatności do obsługi z określonym priorytetem,
    b. przydzielenia nowej podatności do obsługi na zasobie krytycznym,
    c. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
    d. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
    e. modyfikacji przydzielonej operatorowi podatności przez innego operatora,
    f. zamknięcia przydzielonej operatorowi podatności przez innego operatora,
    g. przejęcia przydzielonej operatorowi podatności przez innego operatora.
95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:
    a. wybór raportu który ma zostać wysłany,
    b. zdefiniowanie jego tytułu,
    c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
    d. możliwość ograniczenia cyklu do dni powszednich,

e. określenie daty przesłania pierwszego raportu,
f. określenie okresu przez jaki będą one przesyłane, poprzez:
   - zdefiniowanie daty końcowej,
   - bez daty końcowej,
   - określenie liczby raportów,
g. określenie odbiorców raportu.

96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard'u", tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika.
97. System musi pozwalać na tworzenie dedykowanych dashboard'ów obejmujących:
    a. zestaw wykresów dla bieżącego użytkownika,
    b. zestaw wykresów dla wybranego użytkownika,
    c. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
    d. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).
98. System musi zapewniać zestaw predefiniowanych dashboard'ów obejmujących następujące wykresy:
    a. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:
       - ilość zdarzeń nowych i niesklasyfikowanych,
       - ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
       - ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,
    b. wykres przedstawiający skale zagrożeń, który uwzględnia:
       - ilość zasobów krytycznych na których są obsługiwane zdarzenia,
       - ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,
    c. wykres przedstawiający źródła zagrożeń, który uwzględnia:
       - ilość nowych zdarzeń dotyczących użytkowników,
       - ilość podjętych zdarzeń dotyczących użytkowników,
       - ilość nowych zdarzeń dotyczących zasobów,
       - ilość podjętych zdarzeń dotyczących zasobów,
    d. wykres przedstawiający poziom zagrożeń, który uwzględnia:
       - ilość nowych zdarzeń w podziale na priorytety,
       - ilość podjętych zdarzeń w podziale na priorytety,
    e. wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:
       - ilość zdarzeń zarejestrowanych w bieżącym dniu,
       - ilość zdarzeń zarejestrowanych w ostatnim tygodniu,
       - ilość zdarzeń zarejestrowanych w ostatnim miesiącu,
       - ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,
    f. wykres przedstawiający zagrożone usługi, który uwzględnia:
       - ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
       - ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,
       - wykres przedstawiający zagrożone dane, który uwzględnia:
       - ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
       - ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
       - ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
       - ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
    g. wykres przedstawiający skale podatności, który uwzględnia:
       - ilość zasobów krytycznych na których są obsługiwane podatności,
       - ilość zasobów niekrytycznych na których są obsługiwane podatności,
    h. wykres przedstawiający czas obsługi podatności, który uwzględnia:
       - ilość podatności zarejestrowanych w bieżącym dniu,
       - ilość podatności zarejestrowanych w ostatnim tygodniu,

- ilość podatności zarejestrowanych w ostatnim miesiącu,
- ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,

i. wykres przedstawiający wagę podatności, który uwzględnia:
- ilość nowych podatności w podziale na priorytety,
- ilość podjętych podatności w podziale na priorytety,

99. Nawigacja w ramach „Dashboard'u" musi wspierać opcję typu „Drill down" w następującym zakresie:
   a. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
   b. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
   c. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
   d. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
   e. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
   f. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres.
100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.
101. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego.
102. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć.
103. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.
104. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie.
105. Produkt musi umożliwiać równoczesną pracę co najmniej 5 operatorów oraz obsługiwać 200 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.
106. Dla wszystkich źródeł objętych licencją oraz stanowiących jednocześnie komputery bądź serwery licencja produktu musi uwzględniać możliwość wykorzystania dedykowanych agentów XDR.
107. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.
108. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise", w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

109. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
110. Dostarczone rozwiązanie musi być objęte 36 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).
111. Wykonawca udzieli Zamawiającemu wieczystej (perpetual), nieograniczonej czasowo licencji na zakupiony System.

6.2. Oprogramowanie do zarzadzania infrastrukturą IT – licencja szt. 1 – wymagania minimalne

1. Architektura / budowa
   - 1.1. Licencja bezterminowa na oprogramowanie powinna objąć wszystkie stanowiska komputerowe z 36 miesięcznym wsparciem serwisowym.
   - 1.2. System musi posiadać następującą architekturę:
     - 1.2.1. Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
     - 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).
     - 1.2.3. Panel pracownika – aplikacja webowa dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.
     - 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.
     - 1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
     - 1.2.6. Komponenty Agent, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja agentów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.
     - 1.2.7. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.
     - 1.2.8. Agent do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.
     - 1.2.9. Agent musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku msi.

1.2.10. Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.
1.2.11. System musi posiadać możliwość wygenerowania instalatora Agenta, który nie będzie wymagał uprawnień administracyjnych do zainstalowania.
1.2.12. Agent musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).
1.2.13. System powinien umożliwiać generowanie unikatowego identyfikatora agenta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.
1.2.14. Agent musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.
1.2.15. Agent musi wspierać do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu agenta.
1.2.16. System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.
1.2.17. System musi mieć możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów.
1.2.18. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System musi prezentować historię przeprowadzonych konserwacji/utrzymania.

2. Wymagania systemowe
2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera).
2.2. Agent musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11.
2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2012/2012R2/2016/2019/2022, Windows 10) oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.
2.5. Baza danych musi działać na silniku Microsoft SQL Server 2012/2014/2016/2017/2019 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).
2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

3. Interfejsy
3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
3.2. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.

3.3. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.
3.4. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.
3.5. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z dowolnego źródła danych o dowolnej strukturze danych z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.
3.6. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.

4. Funkcjonalności systemu zarządzania infrastrukturą IT
4.1. Funkcjonalność agenta
4.1.1. System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego), uruchamiania i wyłączania polityk w obszarze bezpieczeństwa (DLP).
4.1.2. Agent musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość
4.1.3. Agent musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej a konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.
4.1.4. Agent musi mieć budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agenta.
4.1.5. Po wykryciu nieprawidłowości w pracy dowolnego z modułów Agent powinien podjąć samoczynną próbę jego naprawy i przywrócenia do działania.
4.2. Funkcjonalność konsoli administracyjnej.
4.2.1. Konsola musi być w pełni polskojęzyczna oraz dodatkowo posiadać wersje angielską.
4.2.2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).
4.2.3. Konsola administracyjna musi posiadać dashboardy – dashboard użytkownika, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.
4.2.4. Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór dowolnego widgetu.
4.2.5. Dashboard prezentujący parametry sieci zawiera widgety pogrupowane w kategorie: Czat, Gry, Peer to peer, Streaming, Usługa podstawowa, Usługa podstawowa (szyfrowana), Złośliwe oprogramowanie.
4.2.5.1.1. Lista monitorowanych usług: AIM/ICQ, Back Orifice, Bagle.B, Bagle.h, BGMP, BGP, BitTorrent, Blaster, Blizzard's Battle.net, Call of Duty, Dabber, DHCPv6 (client), DHCPv6 (server), Direct Connect, DNS, Doom, Emule, FTP (connection control), FTP (data port), FTPS (TLS/SSL)(connection control), FTPS (TLS/SSL)(data port), GameSpy Arcade, Gnutella, Gopher protocol, HTTP, HTTP Proxy, HTTPS, IMAP, IMAPS, IMAPv3, iperf, IRC, IRC, iSCSI, Jedi Knight: Jedi Academy, Kazza, Kerberos, Killing Floor, LDAP, LDAP (SSL), LDP, LogMeIn Hamachi, MMP, MPP, MS Exchange Routing, MS Media Server, MS SQL Server (monitor), MS SQL Server (server), MSDP, MSN, Mu Online, Mxit, MySQL, Nessus, NetBIOS (Datagram Service), NetBIOS (Name Service), NetBIOS (Session Service), NetBus, NFS, Niektóre gry firmy Blizzard, Nintendo Wi-Fi Connection, NNTP, NNTP (TLS/SSL), NTP, OpenVPN, POP3, POP3S, PostgreSQL, PPTP, Printer-IPP, Printer-RAW, Print-spooler, Radio internetowe, Rbot/Spybot, RDP, rsyns, RTCP, RTP, RTSP, Sasser, SFTP, SIP, SIP(TLS), SLP,

SMB, SMTP,SMTPS, SNMP, SOCKS proxy, SSH, Steam, Structured Query Language (SQL) Services, Sub7, Symantec System Center agent, TACACS, TeamViewier, Telenet (TLS/SSL), Telnet, TSP, UUCP, VMware Server, VMware VAMI, WASTE, WHOIS, WINS, XMPP/Jabber, Yahoo,! Messenger.

4.2.5.1.2. Dla każdej z usług prezentowane są relacje do wszystkich komputerów zawierające połączenia: powolne, nieosiągalne, rozłączone i poprawne wraz z czasami połączeń.

4.2.6. Dashboard prezentujący informacje o bezpieczeństwie zawiera widgety zawierające informacje: błędy serwera zadań, błędy smart, komputery bez bitlockera, komputery bez połączenia z serwerem, komputery z błędami typu critical / error / warning, duży transfer sieciowy, komputery bez agenta, komputery offline, komputery online, komputery z naruszoną polityką dlp, komputery z nieaktualną polityką dlp, liczba administratorów lokalnych w systemie (online), logowanie w godzinach nocnych, monitorowanie transferu do dysków chmurowych , nieautoryzowana pamięć usb, nowe komputery, nowe urządzenia w sieci, oprogramowanie zabronione, przekroczone cal, przekroczone licencje, subskrypcje, które wygasły, systemy bez wsparcia, wielokrotne logowanie, wysokie użycie cpu, wysokie użycie ram, zaległe szkolenia wideo, zaległe wiadomości elearning, zbyt mało miejsca na hdd, zmiany na kontach użytkowników, zmiany tcp/ip.

4.2.7. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.

4.2.8. Dane na widgetach muszą być aktualizowane automatycznie nie rzadziej niż 1 raz/ godzinę lub w każdym czasie na życzenia użytkownika.

4.2.9. Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany przez min. 5 widgetów (np. w obszarze zarządzania komputerami system powinien być wyposażony w widgety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń)

4.2.10. Z każdego widgetu można uzyskać szczegółową informację analityczną (listę z danymi składającymi się na wybraną wartość na widgecie).

4.2.11. System musi posiadać filtr roboczy, przeszukujący całą tabelę po zdefiniowanym słowie.

4.2.12. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widgety, ich konfigurację i kolejność).

4.2.13. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator agenta, strukturę organizacyjną, stan agenta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku.

4.2.14. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.

4.2.15. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.

4.2.16. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w

Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.

4.2.17. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).

4.2.18. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.

4.2.19. Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL).

4.2.20. Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator (np. Dell)

4.2.21. Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.

4.3. Funkcjonalność panelu pracownika

4.3.1. Automatyczne uruchamianie panelu w momencie zalogowania użytkownika do systemu operacyjnego.

4.3.2. Zakres informacji w panelu jest definiowany przez administratora w formie schematów przypisywanych dla wybranych grup pracowników.

4.3.3. Panel pracownika użytkowany przez kierownika zawiera dodatkowo dane dostępne w panelach podległych pracowników w formie danych skumulowanych i analitycznych.

4.3.4. Wszelkie informacje udostępniane w panelu pracownika pogrupowane są w logiczne sekcje, z możliwością indywidulanego bądź grupowego włączania / wyłączania (ukrywania) sekcji.

4.3.5. Sekcje informacyjne panelu pracownika

4.3.5.1. Zalogowany użytkownik – imię i nazwisko, IP, nazwa komputera, informacje z AD – nazwa domenowa, nr telefonu, nr telefonu komórkowego, stanowisko

4.3.5.2. Dashboard

4.3.5.2.1. Mój komputer – wykorzystanie RAM, dysku, CPU.

4.3.5.2.2. Wiadomości – lista ostatnich wiadomości przesłanych pracownikowi.

4.3.5.3. Sprzęt

4.3.5.3.1. Komputery przypisane do pracownika (nr seryjny, MAC, IP, data ostatniego logowania).

4.3.5.3.2. Komputery używane przez pracownika (nr seryjny, MAC, IP, data ostatniego logowania).

4.3.5.3.3. Urządzenia przypisane przez pracownika (nr seryjny, typ, IP).

4.3.5.3.4. Urządzenia używane przez pracownika (nr seryjny, typ, IP).

4.3.5.4. Oprogramowanie

4.3.5.4.1. Lista używanego oprogramowania (nazwa aplikacji, wersja, Producent, użycie 2 okresi ostatnich 3, 6, 12 miesięcy, data ostatniego uruchomienia).

4.3.5.5. Wiadomości

4.3.5.5.1. Lista wiadomości przesłanych do użytkownika (data, typ wiadomości, nadawca, treść).

4.4. Zarządzanie licencjami

4.4.1. System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).

4.4.2. System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej.

4.4.3. Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania.

4.4.4. System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania”, które definiują 3 kategorie oprogramowania: „oprogramowanie

standardowe" – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe" - pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone" – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze.

4.4.5. System umożliwia zdefiniowanie listy aplikacji zabronionych.

4.4.6. System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu).

4.4.7. System musi umożliwiać zdefiniowanie dowolnej kategorii oprogramowania/pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii.

4.4.7.1. W oparciu o Machine learning system umożliwia analizę procesów oraz przypisanie im odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem uruchamianych procesów.

4.4.7.2. Automatyczne przypisanie kategorii do każdego uruchomionego procesu.

4.4.7.3. Niezależność od zewnętrznych dostawców bazy wzorców procesów.

4.4.8. System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).

4.4.9. System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam gdzie jest to tylko technicznie możliwe.

4.4.10. System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User.

4.4.11. System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.

4.4.12. System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji.

4.4.13. System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.

4.4.14. System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki).

4.4.15. System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł.

4.4.16. System prezentuje datę instalacji oprogramowania.

4.4.17. System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.

4.4.18. System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych).

4.4.19. System umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu).

4.4.20. System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia.

4.4.21. System musi automatycznie wyliczać przybliżone oszczędności z zakupionych a nie zainstalowanych aplikacji, przybliżone oszczędności z zainstalowanych a niewykorzystanych licencji oraz przybliżone nakłady konieczne na uzyskanie pełnej legalności.

4.4.22. System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.

4.4.23. System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach.
4.4.24. System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.
4.4.25. System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.

4.5. Wzorce aplikacji i pakietów
4.5.1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 3,5 tys. wzorców aplikacji, 1,3 tys. producentów, 21 tys. plików, 1,5 tys. wbudowanych treści umów licencyjnych różnych producentów oprogramowania.
4.5.2. System musi udostępniać informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja.
4.5.3. System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania.
4.5.4. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.
4.5.5. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.
4.5.6. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.
4.5.7. System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.).

4.6. Inwentaryzacja sprzętu komputerowego
4.6.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).
4.6.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.
4.6.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).
4.6.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.
4.6.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.
4.6.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).
4.6.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).
4.6.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.
4.6.9. System musi umożliwiać skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach, czy konto jest włączone, zablokowane, czy wymagana jest zmiana hasła, czy hasło wygasa, czy hasło jest wymagane).
4.6.10. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.

4.6.11. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).
4.6.12. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne.
4.6.13. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
4.6.14. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)
4.6.15. System umożliwia dodawanie notatek do każdej pozycji sprzętu.
4.6.16. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
4.6.17. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
4.6.18. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja).

4.7. Inwentaryzacja urządzeń podłączanych do komputera
4.7.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.
4.7.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.
4.7.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).

4.8. Inwentaryzacja urządzeń innych niż komputery
4.8.1. System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switche, routery, monitory, pamięci masowe itp.
4.8.2. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.
4.8.3. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
4.8.4. System musi zbierać informacje o jakości połączenia:
4.8.4.1. Czas odpowiedzi serwisów (usług) podawany w milisekundach:
4.8.4.1.1. Średni czas odpowiedzi.
4.8.4.1.2. Minimalny czas odpowiedzi.
4.8.4.1.3. Maksymalny czas odpowiedzi.
4.8.4.2. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.
4.8.5. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta, a w przypadku, gdy takiego agenta nie posiadają powinien umożliwić zdalną instalację agenta.
4.8.5.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci
4.8.5.2. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.
4.8.6. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.
4.8.6.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.
4.8.7. System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych.
4.8.8. System musi monitorować zmiany ewidencyjne i ruchy sprzętu.
4.8.9. System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.
4.8.10. System musi mieć możliwość przypominania o upływającym terminie gwarancji.
4.8.11. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.
4.8.12. System udostępnia informację o wartości wprowadzonego sprzętu.

4.8.13. System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.

4.8.14. System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.

4.8.15. System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje).

4.9. Zdalna administracja komputerami

4.9.1. System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.

4.9.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.

4.9.3. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.

4.9.4. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).

4.9.5. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).

4.9.6. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.

4.9.7. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.

4.9.8. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu).

4.9.9. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.

4.9.10. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.

4.9.11. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).

4.9.12. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. System posiada co najmniej 70 predefiniowanych poleceń.

4.9.13. System musi umożliwiać zdalne połączenia do wielu komputerów jednocześnie, podgląd i operowanie na pulpitach tych komputerów w technologii WEBRTC.

4.9.14. System musi umożliwiać za pomocą technologii WEBRTC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalację oprogramowania, poprawek i aktualizacji (service pack, patch).

4.9.15. System musi umożliwiać poprzez technologię WEBRTC zdalne zarządzanie plikami (tworzenie, kopiowanie, usuwanie, przesyłanie) i wykorzystanie wiersza poleceń (cmd) oraz powershell bez konieczności podłączenia do komputera.

4.9.16. System musi umożliwiać nagrywanie sesji połączeń WEBRTC jak i nawiązywanie komunikacji z użytkownikiem podczas sesji (czat).

4.9.17. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.9.18. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.10. Automatyzacja

4.10.1. System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.

4.10.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.

4.10.3. System musi mieć możliwość definiowania czynności wykonywanych automatycznie.

4.10.4. System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).

4.10.5. System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji,

4.10.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).

4.10.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)

4.10.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.

4.10.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.

4.10.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.

4.11. Zarządzanie magazynem IT

4.11.1. System musi umożliwiać obsługę magazynu IT.

4.11.2. System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach.

4.11.3. System musi umożliwiać obsługę dokumentów PZ, WZ, MM+, MM-, LI.

4.11.4. System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło).
4.11.5. System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach.
4.11.6. System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie.

4.12. Repozytorium
4.12.1. Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.
4.12.2. Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.

4.13. Kody kreskowe
4.13.1. System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych.
4.13.2. System wspiera parametryzację kodu w zakresie wielkości graficznej kodu.
4.13.3. System pozwala w każdym momencie na zmianę typu i atrybutów kodu.
4.13.4. System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.
4.13.5. Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów.
4.13.6. System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.
4.13.7. Obsługa kodów kreskowych nie może wymagać instalacji czcionek.
4.13.8. Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne.
4.13.9. System musi umożliwiać współpracę z zewnętrznymi czytnikami kodów.

4.14. System szkolenia pracowników za pomocą wiadomości.
4.14.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.
4.14.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa", „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa", „Postępowanie w przypadku naruszenia tajemnicy", „Udostępnienie informacji stanowiących tajemnicę".
4.14.3. Formatowanie treści musi być zgodne z HTML.
4.14.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).
4.14.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.
4.14.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.
4.14.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.
4.14.8. System musi posiadać zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy) odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalające na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości.
4.14.9. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.
4.14.10. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).
4.14.11. System musi posiadać możliwość eksportu / importu treści.

4.15. Monitorowanie drukarek sieciowych i wydruków

4.15.1. System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).
4.15.2. Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.
4.15.3. System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru.
4.15.4. System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.
4.15.5. System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy.
4.15.6. System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników.
4.15.7. Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych

4.16. Monitorowanie stron www
4.16.1. System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.
4.16.2. Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.
4.16.3. Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).
4.16.4. Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności.
4.16.5. W oparciu o algorytmy sztucznej inteligencji - machine learning oraz deep learning system umożliwia analizę treści rtcstron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron.
4.16.6. Każda odwiedzona strona otrzymuje atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna.

4.17. Monitorowanie dziennika zdarzeń
4.17.1. System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.
4.17.2. Ewidencja zdarzeń musi następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system.
4.17.3. System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.
4.17.4. Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.
4.17.5. System musi umożliwiać monitorowanie komunikatów Syslog.

4.18. Monitorowanie pracy komputerów
4.18.1. System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.
4.18.2. System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.
4.18.3. System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie

4.19. Monitorowanie sesji zdalnych połączeń
- 4.19.1. System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze.
- 4.19.2. Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia.

4.20. Repozytorium CMDB – centralna baza systemu umożliwiająca import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta, na którą składają się:
- 4.20.1. Active Directory - lista skonfigurowanych z konsolą serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System pozwala na wprowadzanie dowolnej ilości serwerów dla różnych domen.
- 4.20.2. Kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania.
- 4.20.3. Kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje.
- 4.20.4. Budżet - zestawienie typów budżetów (kosztów) zaewidencjonowanych w systemie.
- 4.20.5. Komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera.
- 4.20.6. Dokumenty - repozytorium dokumentów zapisanych w systemie.
- 4.20.7. eLearning - zdefiniowane wiadomości typu eLearning. Wykorzystywane są do wysyłania użytkownikom szkoleń wbudowanych w system, zgodnie ze zdefiniowanym harmonogramem.
- 4.20.8. Kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski.
- 4.20.9. Pliki - lista zinwentaryzowanych plików ze wszystkich komputerów.
- 4.20.10. Licencje - zestawienie licencji zapisanych w bazie systemu, które administrator może przypisywać do poszczególnych użytkowników.
- 4.20.11. Typy licencji - lista typów licencji.
- 4.20.12. Lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. W odróżnieniu od struktury organizacyjnej dane nie są importowane z Active Directory.
- 4.20.13. Typy urządzeń - lista typów urządzeń.
- 4.20.14. Urządzenia - lista urządzeń podzielonych wg typu.
- 4.20.15. Producenci / Dostawcy - lista producentów i dostawców.
- 4.20.16. Pamięć masowa - zestawienie dysków twardych z komputerów.
- 4.20.17. Porty sieciowe - lista monitorowanych portów sieciowych.
- 4.20.18. Usługi sieciowe - lista monitorowanych usług sieciowych.
- 4.20.19. Udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych.
- 4.20.20. Sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery.
- 4.20.21. Systemy operacyjne - zestawienie unikalnych systemów operacyjnych.
- 4.20.22. Struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory.
- 4.20.23. Kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji.
- 4.20.24. Serwery - lista zinwentaryzowanych serwerów.
- 4.20.25. Usługi - zestawienie usług działających na komputerach.
- 4.20.26. Oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania.
- 4.20.27. Pamięć masowa USB - lista urządzeń pamięci masowej USB.
- 4.20.28. Administratorzy - lista administratorów systemu,
- 4.20.29. Użytkownicy / pracownicy - lista pracowników.

  Kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję.

4.21. Worktime manager

4.21.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.
4.21.2. Dane muszą być prezentowane w formie interaktywnych widgetów oraz w formie danych analitycznych.
4.21.3. Dane dla grup użytkowników muszą być skumulowane oraz analityczne.
4.21.4. Prezentacja danych odbywa się poprzez wskazanie pracownika lub grupy pracowników oraz wybranie okresu danych źródłowych.
4.21.5. Informacje dotyczące prezentowane w panelu to informacja o otwartych sesjach, informacja o sesjach historycznych, informacja o czasie zalogowania użytkownika, informacja o czasie pracy komputera, informacja o aktywności użytkownika w aplikacjach, informacja o produktywności użytkownika w aplikacjach, informacja o produktywności, wykorzystywanych aplikacjach, odwiedzonych stronach www z podziałem na kategorie stron, informacja o uruchomionych procesach z podziałem na kategorie, informacja o aktywności na stronach www, informacja o wykonanych wydrukach (nazwa dokumentu, data i godzina wydruku, drukarka, ilość stron, rodzaj wydruku – czarno-biały czy w kolorze, koszt wydruku), informacja o transferze sieciowym, informacja o zależności czasu pracy w trybach: zalogowany/ uśpiony/ wylogowany.
4.21.6. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.
4.21.7. System musi prezentować w formie tabelarycznej informacje o dokumentach (np. protokoły przekazania i zwrotu sprzętu), komputerach i urządzeniach, które zostały przypisane użytkownikowi.
4.21.8. System musi posiadać widgety prezentujące dane w wybranym przedziale czasu: czas zalogowania – dni, czas pracy komputera – dni, aktywność w aplikacjach, produktywność w aplikacjach, produktywność w czasie pracy, czas pracy w aplikacjach, czas spędzony na stronach www wg kategorii stron, czas spędzony w aplikacjach (procesach) wg kategorii procesu, czas aktywność na stronach www, stron wydruku wg dokumentów, transfer sieciowy, czas pracy wg zalogowany/ wylogowany / uśpiony, czas aktywności w godzinach pracy.

4.22. Raportowanie i eksport danych
4.22.1. Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.
4.22.2. System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).
4.22.3. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.
4.22.4. Generowanie raportu musi odbywać się po stronie serwera, a nie klienta.
4.22.5. System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).
4.22.6. System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt).
4.22.7. System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF.
4.22.8. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).
4.22.9. System musi posiadać co najmniej 150 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych.
4.22.9.1. Raporty z zakresu komputerów
- Komputery – Karta graficzna – Procesor
- Komputery – Serwery wg systemu operacyjnego
- Komputery wg procesora – Skrócony
- Komputery wg procesora – Wszystkie
- Komputery wg producenta – Skrócony
- Komputery wg producenta – Wszyscy
- Komputery wg struktur organizacyjnych – Skrócony

- Komputery wg struktury organizacyjnej – Wszystkie
- Komputery wg systemów operacyjnych – Skrócony
- Komputery wg systemów operacyjnych – Wszystkie
- Komputery wg typu – Desktop
- Komputery wg typu – Hyper-V
- Komputery wg typu – Mobile
- Komputery wg typu – Nieokreślone
- Komputery wg typu – Server
- Komputery wg typu – Virtual Machine
- Komputery wg typu – VMWare
- Komputery wg typu – Wszystkie typy
- Zestawienie komputerów wg typu – Skrócony
- Komputery online
- Komputery niezautoryzowane
- Komputery offline
- Komputery online
- Komputery w magazynie
- Komputery w naprawie
- Komputery wszystkie
- Komputery wycofane
- Komputery zablokowane
- Komputery zautoryzowane
- Komputery zlikwidowane
- Komputery z Intel Anti-Theft
- Komputery z Intel VPro

4.22.9.2. Raporty z zakresu urządzeń

- Urządzenia – Notatki
- Urządzenia – USB – Dodane
- Urządzenia – USB – Wykryte
- Urządzenia – USB – Wszystkie
- Urządzenia – USB – Biała lista
- Urządzenia – Serwis
- Urządzenia – Inwentaryzacja – Kody kreskowe
- Urządzenia – Inwentaryzacja
- Urządzenia – Inwentaryzacja – Porównanie inwentaryzacji
- Urządzenia – Utrzymanie
- Urządzenia

4.22.9.3. Raporty z zakresu sieci

- Sieć – Wykryte
- Sieć – Historia
- Sieć – Ostanie skanowanie

4.22.9.4. Raporty z zakresu oprogramowania

- Oprogramowanie – Systemy operacyjne – Wszystkie
- Oprogramowanie – Systemy operacyjne – Instalacje OEM
- Oprogramowanie – Systemy operacyjne – Szczegóły
- Oprogramowanie – Systemy operacyjne – Historia audytów
- Oprogramowanie – Aplikacje – Wszystkie
- Oprogramowanie – Aplikacje – Monitorowane
- Oprogramowanie – Aplikacje – Szczegóły
- Oprogramowanie – Aplikacje – Historia audytów
- Oprogramowanie – Pakiety – Wszystkie
- Oprogramowanie – Pakiety – Szczegóły
- Oprogramowanie – Pakiety – Historia audytów
- Oprogramowanie – Bazy danych – Wszystkie

- Oprogramowanie – Bazy danych – Express
- Oprogramowanie – Bazy danych – Pozostałe
- Oprogramowanie – Bazy danych – per Core
- Oprogramowanie – Rejestry – Razem
- Oprogramowanie – Rejestry – Szczegóły
- Oprogramowanie – Rejestry – Ostatnio zainstalowane
- Oprogramowanie – Klucze produktu
- Oprogramowanie – Wykorzystanie – Użycie – Wszystkie
- Oprogramowanie – Wykorzystanie – Oszczędności
- Oprogramowanie – Wykorzystanie – CAL
- Oprogramowanie – Wykorzystanie – CAL WEB
- Oprogramowanie – Monitorowanie – Uruchomienia
- Oprogramowanie – Monitorowanie – Aktywność ogółem

4.22.9.5. Raporty z zakresu osób
- Osoby – Protokół standardowy
- Osoby – Protokół rozszerzony

4.22.9.6. Raporty z zakresu plików i multimediów
- Pliki i multimedia – Archiwa
- Pliki i multimedia – Audio
- Pliki i multimedia – Erotyka
- Pliki i multimedia – Grafika
- Pliki i multimedia – Wideo
- Pliki i multimedia – Wykonywalne
- Pliki i multimedia – Zmiany plików

4.22.9.7. Raporty z zakresu magazynu
- Magazyn – Dokumenty
- Magazyn – Stany
- Magazyn – Materiały
- Magazyn

4.22.9.8. Raporty z zakresu finansów
- Finanse – Urządzenia
- Finanse – Licencje
- Finanse – Wydruki wg drukarki
- Finanse – Wydruki wg sterownika
- Finanse – Wydruki użytkownicy
- Finanse – Magazyn

4.22.9.9. Raporty z zakresu serwera wiadomości
- Serwer wiadomości – Komunikator – Historia
- Wiadomość cykliczna – wg wiadomości
- Serwer wiadomości – Komunikator – Rozmowy
- Serwer wiadomości – Wiadomości wysłane – wg komputera
- Serwer wiadomości – Wiadomości wysłane – wg odbiorcy
- Serwer wiadomości – Wiadomości wysłane – wg wiadomości
- Serwer wiadomości – Wiadomości wysłane – wg wysyłającego
- Serwer wiadomości – Wiadomości – Aktywne cykle

4.22.9.10. Raporty z zakresu serwera monitorującego
- Serwer monitorujący – Logowanie agentów
- Serwer monitorujący – eServer
- Serwer monitorujący – Alerty systemowe
- Serwer monitorujący – Historia logowań
- Serwer monitorujący – Dzienniki zdarzeń – Powiadomienia systemowe
- Serwer monitorujący – Dzienniki zdarzeń – Dzienniki
- Serwer monitorujący – Dzienniki zdarzeń – Sesje RDP
- Serwer monitorujący – Transfer sieciowy – Procesy

- Serwer monitorujący – Drukowanie
- Serwer monitorujący – Drukowanie – Razem
- Serwer monitorujący – Drukowanie – Razem SNMP
- Serwer monitorujący – Drukowanie – Prognoza
- Serwer monitorujący – Usługi – Wszystkie
- Serwer monitorujący – Usługi – Szczegóły
- Serwer monitorujący – Harmonogram zadań
- Serwer monitorujący – Sesje VNC
- Serwer monitorujący – Intel AMT
- Serwer monitorujący – Strony www – Odwiedzone
- Serwer monitorujący – Strony www – Aktywność ogółem
- Serwer monitorujący – USB
- Serwer monitorujący – Wydajność – CPU
- Serwer monitorujący – Wydajność – Dysk
- Serwer monitorujący – Wydajność – Dysk (razem)
- Serwer monitorujący – Wydajność – Pamięć
- Serwer monitorujący – Wydajność – Procesy
- Serwer monitorujący – Wydajność – Sieć

4.22.9.11. Raporty z zakresu serwera zadań

- Serwer zadań – Logi
- Serwer zadań – Zadania cykliczne

4.22.9.12. Raporty z zakresu serwera automatyzacji

- Serwer automatyzacji – Automaty
- Serwer automatyzacji – Logi

4.22.9.13. Raporty z zakresu raportów

- Raporty – Harmonogram
- Raporty – Harmonogram – Historia

4.22.9.14. Raporty z zakresu repozytorium

- Repozytorium – Dokumenty
- Repozytorium – e-Learning
- Repozytorium – Kategorie aplikacji
- Repozytorium – Kategorie plików
- Repozytorium – Kategorie procesów
- Repozytorium – Kategorie www
- Repozytorium – Producenci Dostawcy
- Repozytorium – Typy licencji
- Repozytorium – Zdalna instalacja – Repozytorium
- Repozytorium – Zdalna instalacja – Logi

4.22.9.15. Raporty z zakresu ustawień

- Ustawienia – Administratorzy – Wszystkie
- Ustawienia – Dane firmy
- Ustawienia – Struktura organizacyjna
- Ustawienia – Budżet
- Ustawienia – Sieci

4.22.10. System musi posiadać możliwość ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu.

4.22.10.1. Wynikiem wykonania harmonogramu jest raport w formacie pdf.

4.22.10.2. Harmonogram można skonfigurować.

4.23. Powiadomienia

4.23.1. System musi umożliwiać generowanie powiadomienia w formie alertu w konsoli systemu, wiadomości email wysłanej na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów.

4.23.2. System musi umożliwiać tworzenie wybranych powiadomień wiele razy z określeniem innych grup obiorców

4.23.3. System musi umożliwiać edycję treści wysyłanych powiadomień i możliwość korzystania z danych umieszczonych w systemie w treści powiadomienia.

4.23.4. System musi posiadać co najmniej 30 zdefiniowanych powiadomień dotyczących obszarów funkcjonalnych

4.23.5. Powiadomienia z zakresu oprogramowania

- Odinstalowano oprogramowanie
- Wykryto niezgodność ze schematem oprogramowania
- Wykryto nowe oprogramowanie

4.23.6. Powiadomienia z zakresu sieci

- Monitorowana usługa sieciowa przestała odpowiadać
- Monitorowane urządzenia z problemami
- Monitorowane urządzenie jest offline
- Problem ze stroną WWW
- Serwis WWW nie odpowiada
- Serwis WWW odpowiada niewłaściwym komunikatem
- Średni czas odpowiedzi usługi przekroczył wartość X ms
- Transfer sieciowy na komputerze przekroczył X MB / Y min
- W sieci pojawiły się duplikaty adresów IP
- W sieci pojawiły się duplikaty adresów MAC
- Wykryto dużą ilość danych wysyłanych przez dany port w switch'u
- Wykryto nowe urządzenie
- Wykryto urządzenie z odblokowanym portem X
- Wykryto urządzenie z usługą X
- Wykryto zmianę adres IP komputera
- Wykryto zmianę statusów portów w switch'u

4.23.7. Powiadomienia z zakresu sprzętu

- Interfejs sieciowy wyłączony
- Parametr lub parametry S.M.A.R.T. przekroczyły dozwolone wartości
- Podłączono urządzenie USB
- Wykryto zmianę w sprzęcie (WMI)

4.23.8. Powiadomienia z zakresu systemu

- Mało miejsca na dysku C
- Pojawił się błąd w dzienniku zdarzeń Windows
- Wykryto problem z usługą systemu Windows
- Wykryto zmianę nazwy komputera
- Wysokie użycie pamięci RAM
- Zmieniono informację o systemie

4.23.9. Powiadomienia z zakresu użytkownika

- Użytkownik odwiedził stronę WWW z wybranej kategorii
- Użytkownik przekroczył limit wydrukowanych stron
- Użytkownik przekroczył transfer sieciowy X MB / Y min

5. Bezpieczeństwo

5.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.

5.2. Uwierzytelnianie do systemu musi być realizowane:

5.2.1. z wykorzystaniem imiennego konta użytkownika i hasła,

5.2.2. z wykorzystaniem imiennego konta administratorów aplikacji i hasła,

5.2.3. za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory,

5.2.4. za pośrednictwem jednokrotnego uwierzytelniania poprzez CAS,

5.2.5. za pomocą kluczy uwierzytelniających.

5.2.6. za pomocą kodu na maila

5.3. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.

5.4. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych,

ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).

5.5. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.

5.6. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie.

5.7. Uwierzytelnianie za pomocą kluczy

5.7.1. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.

5.7.2. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256.

5.7.3. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019.

5.8. System musi udostępniać historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów.

5.9. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy agentami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.

5.10. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.

5.11. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.

5.12. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).

5.13. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od agentów.

5.14. System musi zapewniać:

5.14.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.

5.14.2. Przechowywanie logów systemowych.

5.14.3. Przechowywanie logów bezpieczeństwa.

5.14.4. Przechowywanie logów aktywności użytkowników i administratorów.

5.14.5. Pobieranie logów z agentów z poziomu konsoli administracyjnej.

5.14.6. Możliwość eksportu logów.

5.14.7. Definiowanie maksymalnego czasu przechowywania plików log.

5.15. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

6. Wsparcie, pomoc, informacje dodatkowe

6.1. System musi posiadać dokumentację w postaci min. 20 filmów instruktażowych/nagrań z webinarów w języku polskim.

6.2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.

6.3. Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

6.4. Zdalne wykonanie instalacji, konfiguracji i profilowanie systemu.

6.5. Minimum 2 godziny szkolenia z obsługi dostarczonego systemu.

Certyfikat dla administratorów przeszkolonych z użytkowania systemu.

6.3. Oprogramowanie do wirtualizacji – licencja szt. 1 – wymagania minimalne

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie minimum 1000 instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
   a. Login i hasło,
   b. Karty z certyfikatami (smartcard),
   c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
   - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
   - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
   - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
   - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
c. Zdalna dystrybucja oprogramowania na stacje robocze.
d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   - Dystrybucję certyfikatów poprzez http
   - Konsolidację CA dla wielu lasów domeny,
   - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f. Szyfrowanie plików i folderów.
g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i. Serwis udostępniania stron WWW.
j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
k. Wsparcie dla algorytmów Suite B (RFC 4869),
l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
   - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   - Obsługi 4-KB sektorów dysków
   - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

6.4. Oprogramowanie do backupu – licencja szt. 1 – wymagania minimalne

Pozycja dotyczy zakupu aktualizacji licencji na posiadany system backupu wraz z aktualizacją wersji do najnowszej oferowanej przez producenta oprogramowania - podniesienie wersji. Veeam Backup Essentials Universal Perpetual License - 30 instancji

Wymagania ogólne

- Minimalna ilość licencji musi umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 20 VM oraz 3 serwerach fizycznych.
- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
- Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
- Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania

- Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
- Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
- Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
- Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
- Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
- Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
- Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
- Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
- Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO

- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
- Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
- Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
- Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
- Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
- Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
- Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
- Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

Wymagania RTO

- Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
- Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
- Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków

- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
- Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
  - Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
  - BSD: UFS, UFS2
  - Solaris: ZFS, UFS
  - Mac: HFS, HFS+
  - Windows: NTFS, FAT, FAT32, ReFS
  - Novell OES: NSS
- Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
- Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
- Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
- Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
- Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
- Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
- Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
- Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
- Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

- Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
- Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
- Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
- Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
- Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Monitoring

- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
- System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez VMware
- System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
- System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
- System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
- System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
- System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
- System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x

Raportowanie

- System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022
- System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
- System musi być certyfikowany przez VMware i posiadać status „VMware Ready"
- System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
- System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
- System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
- System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach

- System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
- System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
- System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
- System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
- System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

6.5. Macierz dyskowa – szt. 1 – wymagania minimalne

Lp.	Nazwa parametru	Wartość parametru
1.	Obudowa	Macierz musi być dostarczona ze wszystkimi komponentami do instalacji w szafie rack 19''.
2.	Pojemność:	Macierz musi zostać dostarczona w konfiguracji zawierającej minimum: 18 dysków SSD o pojemności minimum 1.92TB każdy Macierz musi wspierać dyski: - SSD: od 800GB do 15.3TB Macierz musi mieć możliwość rozbudowy do minimum 120 dysków hot-swap. Macierz musi być macierzą all-flash, nie dopuszcza się macierzy, która może jednocześnie obsługiwać dyski SSD i HDD.
3.	Kontroler	Dwa kontrolery macierzy wyposażone w przynajmniej 32GB cache każdy. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash. Zawartość cache musi być mirrorowana (kopia lustrzana) między kontrolerami.
4.	Interfejsy	Oferowana macierz musi posiadać minimum: - 8 portów 10Gb iSCSI / 16Gb FC obsadzonych wkładkami SFP 10/16Gb, - 4 porty SAS 12 Gb/s do komunikacji z półkami rozszerzeń - 2 porty RJ-45 10/100/1000 Mb Ethernet typu out-of-band management. Macierz musi pozwalać na wymianę portów FC na porty 10/25Gb iSCSI bez potrzeby wymiany kontrolera macierzy.
5.	RAID	Kontrolery macierzy muszą umożliwiać konfigurację dysków w RAID: 0, 1, 5, 6, 10. Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 120 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.
6.	Obsługiwane protokoły	Macierz musi obsługiwać protokoły FC, iSCSI.
7.	Inne wymagania	Macierz musi posiadać wsparcie dla systemów:

		Microsoft Windows Server 2012 R2, 2016, and 2019; Red Hat Enterprise Linux (RHEL) 6, 7, and 8; SUSE Linux Enterprise Server (SLES) 11, 12, and 15; VMware vSphere 6.5, 6.7, and 7.0. Macierz musi posiadać funkcjonalność wykonywania minimum 512 kopii migawkowych typu copy-on-write. Macierz musi posiadać funkcjonalność klonowania danych i replikacji asynchronicznej. Macierz musi mieć możliwość replikacji danych po FC w trybie synchronicznym i asynchronicznym. Macierz musi pozwalać na wykonanie do 32 jednoczesnych replikacji bez używania systemów zewnętrznych wykonujących replikację. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 512 partycji. Macierz musi pochodzić od tego samego producenta co serwery rack objęte niniejszym zapytaniem. Macierz musi posiadać funkcjonalność thin provisioning. Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID. Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji. Macierz musi posiadać oprogramowanie pozwalające na integrację z VMware vCenter. Macierz musi zapewniać możliwość szyfrowania danych przy użyciu dysków typu FIPS SSD. Realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami. Wszystkie licencje (z wyłączeniem replikacji synchronicznej) na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy.
8.	Gwarancja i serwis	Wymagana jest naprawa w trybie NBD. Dyski uszkodzone pozostają u Zamawiającego. Dostarczony system musi posiadać również okres subskrypcji równy gwarancji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.

6.6. Klaster firewall – szt. 1 – wymagania minimalne

Wymagania Ogólne System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.	

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 4 gniazdami SFP+ 10 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.
5. System jest wyposażony w zasilanie AC.
6. Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 2.8 mln. jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 30 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.

Funkcje Systemu Bezpieczeństwa:
W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajno
2. ściowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.
3. Zgłoszenia serwisowe musza być przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

6.7. Centralny system logów – szt. 1 – wymagania minimalne

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 6.5, 6.7; Microsoft Hyper-V wersje: 2019, 2022; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 1TB

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 1 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
   a. Listę najczęściej wykrywanych ataków.
   b. Listę najbardziej aktywnych użytkowników.
   c. Listę najczęściej wykorzystywanych aplikacji.
   d. Listę najczęściej odwiedzanych stron www.
   e. Listę krajów , do których nawiązywane są połączenia.
   f. Listę najczęściej wykorzystywanych polityk Firewall.
   g. Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.

2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.
   - Email.
   - IPS.
   - Traffic.
   - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

Wsparcie: System musi być objęty serwisem przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

6.8. Zestaw komputerowy z oprogramowaniem – szt. 35 – wymagania minimalne

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Komputer	Komputer fabrycznie wbudowany w obudowę monitora. Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.
2.	Obudowa	Obudowa typu All-in-One z możliwością zabezpieczenia fizycznego przez metalową linkę typu Kensington Lock oraz umożliwiająca beznarzędziową wymianę pamięci RAM. Wyposażona w listwę montażową w standardzie VESA 100x100. Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym
3.	Podstawa	Podstawa umożliwiająca regulację jednostki w zakresie co najmniej: - pochylenie przód tył od -5 do 20 stopni - swivel w zakresie 45 stopni w każdą stronę - pivot w zakresie 90 stopni - regulację wysokości w do 110mm
4.	Chipset	Dostosowany do zaoferowanego procesora
5.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 3 złącza M.2 z czego 2 dedykowane dla dysku SSD PCIe. Płyta główna wyposażona w min. 2 sloty pamięci RAM DDR5.

6.	Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark - Multithread Rating wynik co najmniej 25800 pkt. według wyników opublikowanych na stronie https://www.cpubenchmark.net/cpu_list.php Wynik nie starszy niż 90 dni od daty złożenia oferty. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
7.	Pamięć operacyjna	Min. 16GB RAM, Możliwość rozbudowy do min. 64GB Jeden slot pozostawiony wolny
8.	Dysk twardy	Min 512GB M.2 PCIe, wspierający sprzętowe szyfrowanie dysku OPAL, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość instalacji drugiego dysku SSD M.2
9.	Karta graficzna	Zintegrowana karta graficzna z procesorem.
10.	Matryca	Min. 23,8" IPS o rozdzielczości min. FHD 1920x1080 Jasność typowa min. 250 cd/m^2 Kontrast typowy min. 1300:1 Typowy czas reakcji matrycy maksymalnie 14ms Odświeżanie min. 60Hz Gamut min. 99% sRGB Sprzętowa funkcja redukująca emisję światła niebieskiego Kąty widzenia poziomo/pionowo min. 178/178 stopni
11.	Multimedia	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane dwa głośniki o mocy min. 3W każdy Wbudowane dwa mikrofony. Kamera min. 5MP zintegrowana z obudową komputera, z mechaniczną zasłoną obiektywu, funkcją logowania za pomocą rozpoznawania twarzy oraz możliwością regulacji pochylenia w zakresie od -20 do 20 stopni.
12.	Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000 Wbudowana karta sieci bezprzewodowej, pracująca w standardzie AX Bluetooth min. 5.1
13.	Porty/złącza	Z tyłu obudowy: - 1 x USB 3.2 typu C Generacji 2 - 3 x USB 3.2 typu A Generacji 1 - 1 x HDMI combo - 1x DisplayPort 1.4 - 1x RJ-45 Z boku obudowy: - 3x USB 3.2 typu A Generacji 2 - 1x złącze audio combo Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
14.	Klawiatura/mysz	Przewodowa USB: klawiatura w układzie US + mysz z rolką
15.	Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 180W oraz sprawności na poziomie min. 90%.
16.	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1.Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2.Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego

		3.Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4.Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5.Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6.Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7.Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8.Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9.Wbudowany system pomocy w języku polskim. 10.Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11.Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12.Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13.Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14.Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15.Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16.Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17.Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18.Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19.Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20.Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21.Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22.Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23.Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24.Wbudowany mechanizm wirtualizacji typu hypervisor." 25.Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26.Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.

		27.Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28.Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29.Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30.Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31.Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32.Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33.Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34.Możliwość tworzenia wirtualnych kart inteligentnych. 35.Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36.Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37.Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38.Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39.Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40.Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41.Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42.Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43.Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
17.	BIOS	Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera, - numerze seryjnym, - numerze inwentarzowym (AssetTag), - MAC Adres karty sieciowej, - wersji BIOS, - dacie produkcji BIOS - zainstalowanym procesorze, - zainstalowanej pamięci RAM, - urządzeniach podłączonych do portów M.2 Możliwość z poziomu Bios: - wyłączenia/włączenia selektywnego (pojedynczo) portów USB

		- wyłączenia karty sieciowej - wyłączenia karty audio - wyłączenia funkcji Wake on LAN - wyłączenia wirtualizacji - wyłączenia modułu TPM - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, dysku twardego - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania sekwencji bootowania, z uwzględnieniem PXE, zewnętrznych nośników, dysku twardego - załadowania optymalnych ustawień Bios bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
18.	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający wykonanie diagnostyki następujących podzespołów: • test pamięci RAM • test dysku twardego • test portów USB • test płyty głównej • test procesora Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja, data wydania, producent • Procesor : Nazwa, taktowanie, liczba rdzeni, liczba wątków, pamięć cache L1, L2, L3 • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny, taktowanie • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy, producent • System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
19.	Certyfikaty i standardy	Dla komputera: - Deklaracja zgodności CE - TUV Rheinland Low Blue Light - TUV Rheinland Flicker Free - MIL-STD-810H
20.	Bezpieczeństwo	- Złącze typu Kensington Lock - Moduł TPM 2.0 z certyfikacją TCG - Czujik otwarcia obudowy
21.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS

		systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.
22.	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie.
23.	Gwarancja i wsparcie techniczne	Świadczona w miejscu użytkowania sprzętu (on-site). Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej: - fabrycznej konfiguracji urządzenia, - rodzaju gwarancji, - dacie wygaśnięcia gwarancji, - aktualizacjach. Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera.
24.	Pakiet biurowy	Pakiet biurowy spełniający następujące wymagania techniczne: Licencja wieczysta Wymagania odnośnie interfejsu użytkownika: • pełna polska wersja językowa interfejsu użytkownika, • prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; • oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: • posiada kompletny i publicznie dostępny opis formatu, • w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); • do aplikacji musi być dostępna pełna dokumentacja w języku polskim; Pakiet zintegrowanych aplikacji biurowych musi zawierać: • edytor tekstów, • arkusz kalkulacyjny, • narzędzie do przygotowywania i prowadzenia prezentacji, • narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), 1. Edytor tekstów musi umożliwiać: • edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, • wstawianie oraz formatowanie tabel, • wstawianie oraz formatowanie obiektów graficznych, • wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), • automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, • automatyczne tworzenie spisów treści, • formatowanie nagłówków i stopek stron,

		• śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • określenie układu strony (pionowa/pozioma), • wydruk dokumentów, • wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, • wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem, 2. Arkusz kalkulacyjny musi umożliwiać: • tworzenie raportów tabelarycznych, • tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, • tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, • tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService), • obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, • tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, • wyszukiwanie i zamianę danych, • wykonywanie analiz danych przy użyciu formatowania warunkowego, • nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • formatowanie czasu, daty i wartości finansowych z polskim formatem, • zapis wielu arkuszy kalkulacyjnych w jednym pliku, • zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; 3. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: • przygotowywanie prezentacji multimedialnych, • prezentowanie przy użyciu projektora multimedialnego, • drukowanie w formacie umożliwiającym robienie notatek, • zapisanie jako prezentacja tylko do odczytu, • nagrywanie narracji i dołączanie jej do prezentacji, • opatrywanie slajdów notatkami dla prezentera,

		• umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, j) możliwość tworzenia animacji obiektów i całych slajdów, • prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, • pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013, 2016; 4. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: • pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, • filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, • tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • automatyczne grupowanie poczty o tym samym tytule, • tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
25.	Program antywirusowy	**Administracja zdalna w chmurze** 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie,

		cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. **Ochrona stacji roboczych** 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

		16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. **Ochrona serwera** 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

		14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. **Ochrona urządzeń mobilnych opartych o system Android** 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: • usunięcie zawartości urządzenia, • przywrócenie urządzenie do ustawień fabrycznych, • zablokowania urządzenia, • uruchomienie sygnału dźwiękowego, • lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: • nazwę aplikacji, • nazwę pakietu, • kategorię sklepu Google Play, • uprawnienia aplikacji, • pochodzenie aplikacji z nieznanego źródła.

6.9. Laptop z oprogramowaniem – szt. 5 – wymagania minimalne

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Typ	Komputer przenośny.

2.	Procesor	Procesor ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core Ultra 5 125U na podstawie wyników Passmark CPU Mark z dnia XYZ opublikowanych na stronie http://www.cpubenchmark.net/ . Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
3.	Pamięć operacyjna RAM	Min. 16GB DDR5 pracującej w trybie dual channel Możliwość rozbudowy pamięci do min. 64GB
4.	Parametry pamięci masowej	M.2 512 GB SSD PCIe 4.0 x4 NVMe Przygotowana, wolna zatoka do rozbudowy komputera o dodatkowy dysk SSD.
5.	Karta graficzna	Procesor dedykowany do pracy w komputerach przenośnych, osiągający w teście Passmark CPU Mark , w kategorii Average CPU Mark - Multithread Rating wynik co najmniej 17750 pkt. według wyników opublikowanych na stronie https://www.cpubenchmark.net/cpu_list.php Wynik nie starszy niż 90 dni od daty złożenia oferty. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
6.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo 2x2W, port słuchawek i mikrofonu typu COMBO, kamera video 1080p z mechaniczną zasłoną obiektywu oraz obsługująca logowanie za pomocą danych biometrycznych z obsługą między Windows Hello, dwa mikrofony z funkcją wygłuszania niechcianych odgłosów tła, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).
7.	Obudowa	Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane, PC-ABS) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych.
8.	Płyta główna	Płyta główna zaprojektowana i wyprodukowana, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny urządzenia.
9.	Bezpieczeństwo	Moduł fTPM 2.0 lub dTPM 2.0 Slot typu Kensington. Komputery wyposażone w złącze Noble Lock muszą zostać zaoferowane z adapterem ze złącza Noble Lock komputera do Kensington. Dysk systemowy zawierający partycję recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
10.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
11.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - nr seryjnym komputera - typie procesora - ilości pamięci RAM Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość ustawienia hasła administratora - Możliwość ustawienia hasła dysku twardego - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS - Możliwość włączenia/wyłączenia bootowania z USB oraz PXE - Możliwość Wyłączania/Włączania: karty sieciowej, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, USB

12.	Bezpieczeństwo – System Diagonstyczny	Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych: 1. Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów: - pamięci ram, - procesora, - pamięci masowej, - płyty głównej. 2. Identyfikację jednostki i jej komponentów w następującym zakresie: - urządzenie (producent, model, numer seryjny), - bios (producent, wersja oraz data wydania), - procesor (nazwa, taktowanie, ilości pamięci cache), - pamięć ram (ilość zainstalowanej pamięci ram, producent), - dysk twardy (producent, model, numer seryjny, pojemność).
13.	Ekran	Matowy, matryca IPS min. 14” max. 16” 16:10 z podświetleniem w technologii LED, rozdzielczość min. WUXGA 1920x1200, jasność min. 300 nits, kąt otwarcia pokrywy ekranu min. 180 stopni.
14.	Interfejsy / Komunikacja	- 2x USB 3.2 typu A - 1x ThunderBolt 4 - 1x USB 3.2 typu C - 1x HDMI - 1x złącze audio combo - 1x RJ-45 - 1x czytnik kart SD wbudowany lub w formie przejściówki USB Nie dopuszcza się osiągnięcia wymaganych portów USB poprzez zastosowanie przejściówek.
15.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie min. Wi-Fi 6E 11ax Bluetooth min. 5.3
16.	Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, wyposażona w min. 2 tryby podświetlania przycisków (włączone, wyłączone)
17.	Czytnik linii papilarnych	Czytnik linii papilarnych wbudowany w klawiaturę lub przycisk zasilania. Przycisk zasilania znajdujący się poza obrysem klawiatury, celem uniknięcia przypadkowego naciśnięcia. Nie dopuszcza się umiejscowienia przycisku włączania np. w górnym rzędzie klawiatury.
18.	Akumulator	O pojemności min. 45Wh
19.	Zasilacz	Zasilacz zewnętrzny USB-C min. 65W
20.	Certyfikaty, oświadczenia i standardy	Dla komputera: - Deklaracja zgodności CE
21.	Waga	Waga startowa urządzenia nie większa niż 1.75kg według karty katalogowej producenta
22.	System operacyjny	System operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1.Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

		b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2.Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3.Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4.Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5.Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6.Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7.Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8.Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9.Wbudowany system pomocy w języku polskim. 10.Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11.Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12.Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13.Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14.Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15.Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16.Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17.Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18.Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19.Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20.Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21.Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22.Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23.Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24.Wbudowany mechanizm wirtualizacji typu hypervisor." 25.Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26.Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.

		27.Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28.Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29.Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30.Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31.Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32.Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33.Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34.Możliwość tworzenia wirtualnych kart inteligentnych. 35.Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36.Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37.Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38.Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39.Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40.Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41.Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42.Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43.Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
23.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczną weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
24.	Gwarancja i wsparcie techniczne	Gwarancji sprzętu, świadczonej w miejscu użytkowania (on-site). Bezpłatna infolinia w języku polskim, funkcjonująca minimum w godzinach 9:00 – 16:00 oraz obsługująca zgłoszenia serwisowe i oferująca wsparcie techniczne w zakresie co najmniej: - wsparcia technicznego dla zakupionego sprzętu, - weryfikacji konfiguracji fabrycznej zakupionego sprzętu, - weryfikacji statusu gwarancji zakupionego sprzętu. Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej: - fabrycznej konfiguracji urządzenia, - rodzaju gwarancji,

		- dacie wygaśnięcia gwarancji, - aktualizacjach. Diagnostyka sprzętowa dostępna na stronie internetowej producenta
25.	Pakiet biurowy	Pakiet biurowy spełniający następujące wymagania techniczne: • Licencja wieczysta • Wymagania odnośnie interfejsu użytkownika: • pełna polska wersja językowa interfejsu użytkownika, • prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; • oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: • posiada kompletny i publicznie dostępny opis formatu, • w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); • do aplikacji musi być dostępna pełna dokumentacja w języku polskim; Pakiet zintegrowanych aplikacji biurowych musi zawierać: • edytor tekstów, • arkusz kalkulacyjny, • narzędzie do przygotowywania i prowadzenia prezentacji, • narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), 1. Edytor tekstów musi umożliwiać: • edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, • wstawianie oraz formatowanie tabel, • wstawianie oraz formatowanie obiektów graficznych, • wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), • automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, • automatyczne tworzenie spisów treści, • formatowanie nagłówków i stopek stron, • śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • określenie układu strony (pionowa/pozioma), • wydruk dokumentów, • wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, • wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem, 2. Aarkusz kalkulacyjny musi umożliwiać: • tworzenie raportów tabelarycznych, • tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, • tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,

		• tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService), • obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, • tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, • wyszukiwanie i zamianę danych, • wykonywanie analiz danych przy użyciu formatowania warunkowego, • nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • formatowanie czasu, daty i wartości finansowych z polskim formatem, • zapis wielu arkuszy kalkulacyjnych w jednym pliku, • zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; 3. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: • przygotowywanie prezentacji multimedialnych, • prezentowanie przy użyciu projektora multimedialnego, • drukowanie w formacie umożliwiającym robienie notatek, • zapisanie jako prezentacja tylko do odczytu, • nagrywanie narracji i dołączanie jej do prezentacji, • opatrywanie slajdów notatkami dla prezentera, • umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, j) możliwość tworzenia animacji obiektów i całych slajdów, • prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, • pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013, 2016; 4. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: • pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, • filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, • tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • automatyczne grupowanie poczty o tym samym tytule, • tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,

26.	Program antywirusowy	**Administracja zdalna w chmurze** 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. **Ochrona stacji roboczych** 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

		12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. **Ochrona serwera** 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć

		możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. **Ochrona urządzeń mobilnych opartych o system Android** 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: • usunięcie zawartości urządzenia,

		• przywrócenie urządzenie do ustawień fabrycznych, • zablokowania urządzenia, • uruchomienie sygnału dźwiękowego, • lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: • nazwę aplikacji, • nazwę pakietu, • kategorię sklepu Google Play, • uprawnienia aplikacji, • pochodzenie aplikacji z nieznanego źródła.

6.10. UPS – szt. 1 – wymagania minimalne

Lp.	Opis wymagań techniczno-funkcjonalnych	Wartość minimalna
1.	Technologia	VFI (true on-line, podwójne przetwarzanie energii)
2.	Budowa	Beztransformatorowa, prostownik IGBT. UPS musi być wyposażony w podwójny tor zasilający niezależny dla prostownika i Bypassu.
3.	Moc znamionowa	30 kVA / 30kW
4.	Wyjściowy współczynnik mocy (PF)	1,0
5.	Współczynnik mocy wejściowej 0.99.	0,99
6.	Napięcie wejściowe trójfazowe	400 VAC 3F + N
7.	Tolerancja napięcia wejściowego przy obciążeniu 100%; bez przechodzenia na baterie	172 – 287 Vac (L-N)
8.	Zakres częstotliwości wejściowej	Wymagana 40-70 Hz
9.	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 96%
10.	Tryb pracy ECO mode, zapewniający podwyższoną sprawność zasilacza	Wymagany
11.	Możliwość rozbudowy mocy w okresie eksploatacji	Do minimum 8 sztuk w układzie pracy równoległej
12.	Montażu modułu pracy równoległej w oferowanej jednostce	Wymagane – pozwala na dołączenie kolejnej jednostki.
13.	Napięcie wyjściowe trójfazowe	400 VAC 3F + N
14.	Częstotliwość wyjściowa	50/60Hz (programowalna)
15.	Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass)	Statyczny przełącznik (SCR) oraz ręczny rozłącznik serwisowy
16.	Zewnętrzny bezprzerwowy Bypass serwisowy	Wymagany Bypass bezprzerwowy w postaci jednego przełącznika, z informacją o położeniu dla zabezpieczenia falownika UPS przed uszkodzeniem w przypadku nieprawidłowego użycia.
17.	Wejście komunikacyjne na UPS do podłączenia sygnalizacji położenia przełącznika zewnętrznego Bypassu serwisowego, dla ochrony falownika UPS przed przypadkowym przełączeniem	Wymagane
18.	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem.	Wymagane, wraz z funkcją restingu baterii

19.	Możliwość regulacji prądu ładowania baterii z poziomu panelu LCD w UPS-ie.	Wymagane – podać maksymalną wartość prądu ładowania baterii
20.	Czas podtrzymania	6 minut przy obciążeniu 30kW
21.	Minimalna pojemność zainstalowanych akumulatorów liczona jako: Ilosc akumulatorów * pojemność pojedynczego akumulatora * napięcie pojedynczego akumulatora [V*Ah]	8 640 Ah*V
22.	Moduł baterii	Baterie muszą być umieszczone w obudowie UPS. Należy stosować baterie szczelne AGM VRLA o żywotności 10-12 lat. Każdy łańcuch baterii zabezpieczony niezależnym rozłącznikiem bezpiecznikowym.
23.	Autonomia pracy zasilacza UPS przy pracy z baterii podawana w minutach na panelu LCD zasilacza	Wymagane
24.	W przypadku uszkodzenia pojedynczych akumulatorów w stosie, wymagana poprawna praca urządzenia ze zmniejszonym łańcuchem baterii	Wymagane, poprzez konfigurację, zmianę długości łańcucha baterii 30-40 sztuk
25.	Stabilizacja napięcia wyjściowego w stanie ustalonym	± 1%
26.	Stabilizacja napięcia wyjściowego w stanie nieustalonym	± 3%
27.	Stabilność częstotliwości wyjściowej:	bez synchronizacji: ± 0,05 Hz
28.	Współczynnik szczytu	3:1
29.	Minimalne przeciążenie falownika w trybie pracy normalnej	115% przez 60 minut 130% przez 10 minut 150% przez 1 minutę >150% - 0,2 sek
30.	Panel sterujący z wyświetlaczem dotykowym oraz sygnalizacją diodową i akustyczną	Wymagane
31.	Złącze interfejsów	SNMP, Dry Contact In/OUT, Modbus RTU, RS485
32.	Karta sieciowa SNMP wbudowana w UPS.	Wymagane
33.	Interfejs EPO (do wyłącznika ppoż.)	Wymagane – zestyk NO oraz NC. UPS zintegrowany z systemem ppoż budynku.
34.	Diagnostyka parametrów urządzenia UPS i baterii	Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS
35.	Dedykowane oprogramowanie do wysyłania SMS	Wymagane
36.	Poziom hałasu w odległości 1m	< 50 dBA
37.	Rejestr zdarzeń	Dziennik zdarzeń w UPS-ie + komunikaty serwisowe
38.	Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane
39.	Monitorowanie stanu baterii i czasu autonomii	Stan baterii + dostępna autonomia mierzona w czasie rzeczywistym
40.	UPS wyposażony w dotykowy, kolorowy wyświetlacz zabezpieczony hasłem przed ingerencją osób postronnych	Wymagane

41.	UPS wyposażony w programowany tryb pracy ECO mode o podwyższonej sprawności z możliwością zaprogramowania dni tygodnia oraz godzin w jakich UPS przechodzi automatycznie w tryb oszczędnej pracy o podwyższonej sprawności.	Wymagane
42.	UPS wyposażony w funkcję automatycznego czyszczenia z możliwością zaplanowania okresowego samoczynnego załączenia się tej funkcji.	Wymagane
43.	UPS wyposażony w zdalny wyłącznik REPO	Wymagane – dostawa po stronie dostawcy UPS.
44.	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane zarówno dla zasilacza UPS jak i baterii
45.	Rozłączniki manewrowe	Zasilacz UPS powinien być wyposażony w komplet rozłączników pozwalających na bezpieczne włączenie i wyłączenie UPSa. Wymaga się co najmniej czterech rozłączników zamontowanych na UPS: zasilanie prostownika, zasilanie bypass, bypass serwisowy, rozłącznik wyjściowy z UPS.
46.	Podłączenie zasilania i odbiorów	Podłączenie okablowania z tyłu zasilacza, z możliwością podłączenia dwóch oddzielnych torów do zasilania prostownika i bypassu wewnętrznego.
47.	UPS powinien posiadać funkcję umożliwiającą samo dociążenie bez podłączania dodatkowych odbiorników w celu przetestowania podzespołów pod pełnym obciążeniem w trakcie każdej wizyty serwisu.	Wymagane
48.	Zasilacz wyposażony w kółka transportowe pozwalające na łatwe przemieszczanie w czasie konserwacji	Wymagane
49.	Wymiary UPS nie większe niż (S x G x W)	300 x 850 x 1250 mm (+/-5%)
50.	Instrukcja w języku polskim	Wymagane

6.11. Agregat – szt. 1 – wymagania minimalne

1. Moc wg PN-ISO 8528 (+/-5%):
   PRP min. 60 kVA / 48 kW
   LPT (SB) min. 70 kVA / 56 kW
2. Napięcie nominalne: 3x 400 VAC / 50 Hz
3. Prędkość obrotowa: 1500 obr/min
4. Klasa regulacji (ISO 8528-5): G2
5. Regulator silnika: elektroniczny
6. Agregat obudowany i wyciszony o głośności nie większej niż 70 dB z 7 metrów
7. Obudowa wykonana z profili stalowych, ocynkowanych, malowanych proszkowo
8. Maksymalne wymiary obudowy nie większe niż 2500 x 1000 x 1700 mm (D x S x W)
9. Zbiornik paliwa – min. 100l.
10. Drzwi serwisowe po obu stronach obudowy + 1 drzwi do panelu sterowania
11. Dostęp do chłodnicy poprzez przy pomocy zdejmowanego panelu
12. Spawana, stalowa rama agregatu wyposażona w zbiornik paliwa na 12 godzin pracy z pełnym obciążeniem 100% PRP
13. Zamki i okucia obudowy wykonane ze stali nierdzewnej

14. Dwa wskaźniki poziomu paliwa:
    - analogowy, widoczny na zewnątrz obudowy,
    - cyfrowy na panelu sterowania z możliwością wyprowadzenia zdalnego odczytu
15. Wlew paliwa na obudowie, zabezpieczony na klucz
16. Możliwość dotankowania podczas pracy agregatu
17. Agregat wyposażony w układ podgrzewania cieczy chłodzącej umożliwiający start zespołu w niskich temperaturach. Układ podgrzewania musi posiadać termostat umożliwiający regulację zadanej temperatury
18. Tłumiki wibroizolacyjne pomiędzy ramą, a zespołem silnikiem i prądnicą
19. Tłumik wydechu
20. Agregat z bieżącej produkcji, nowy
21. Pompa do spuszczania oleju silnikowego
22. Spalanie silnika Diesla nieprzekraczające 17 l/h przy 100% obciążenia PRP
23. Zalecane przez producenta silnika przeglądy nie częściej niż co 500 motogodzin.
24. Konstrukcja prądnicy: synchroniczna, samowzbudna, samoregulująca, bez-szczotkowa, jednołożyskowa
25. Sprawność prądnicy przy 100% PRP min 88,5 %
26. Panelu automatyki wyposażony w sterownik mikroprocesorowy z cyfrowym wyświetlacz LCD oraz diody sygnalizujące tryb pracy agregatu oraz sieci
27. Panel automatyki posiadający minimum 7 wejść binarnych, 7 wyjść binarnych, 3 wejścia analogowe
28. Panel sterowania przygotowany do pracy w trybach: ręcznym, automatycznym i testowym.
29. Możliwość zastosowania komunikacji zdalnej SNMP oraz MODBUS RTU
30. Wejście do podania sygnału startu i stopu z zewnętrznego układu SZR
31. Możliwość sterowania zewnętrznym układem SZR
32. Menu sterownika w języku polskim
33. Historia zdarzeń sterownika min. 100 wpisów
34. Agregat wyposażony w wyłącznik 3-biegunowy

6.12. Szkolenia TiK typ I – 120 rbh – wymagania minimalne

Pozycja dotyczy przeprowadzenia 3 autoryzowanych przez producenta/wykonawcę szkoleń, w wymiarze 40 godzin każde, z zakresu oprogramowania/sytemu:

1. Administrowania i obsługi systemu operacyjnego (domena, usługa katalogowa) z zakresu zaoferowanego rozwiązania – oprogramowanie domenowe
2. Systemu backupu z zakresu zaoferowanego rozwiązania – oprogramowanie do backupu
3. Systemu wirtualizacji z zakresu zaoferowanego rozwiązania – oprogramowanie do wirtualizacji

Szkolenia/Asysta stanowiskowa ma obejmować 120 godzin szkoleniowych w ujęciu max. 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 15 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.
Asysta musi zostać podzielona na bloki dziedzinowe:

- Blok pierwszy (10 dni – 80 godzin) musi zostać przeprowadzony w centrum kompetencyjnym (poza terenem Zamawiającego) i mieć na celu zapoznanie uczestników z elementami technologicznymi, które składają się na całość autorskiego rozwiązania.
- Blok drugi (5 dni – 40 godziny) musi zostać przeprowadzony w miejscu instalacji (Urzędzie Gminy) i musi ściśle dotyczyć podstawowych procedur administracyjnych, które są typowe dla codziennej pracy administratora celem zapewnienia poprawnej pracy rozwiązania sprzętowego jako platformy teleinformatycznej na potrzeby rozwiązania związanego z oprogramowaniem systemu.

Zakres asysty stanowiskowej:

- Architektura serwerowa;
- Architektura macierzowa;
- Architektura sieci LAN;
- System wirtualizacji danych;
- System backupu i replikacji danych;
- Administrowania i obsługi systemu operacyjnego (domena, usługa katalogowa) z zakresu zaoferowanego rozwiązania – oprogramowanie domenowe.
- Punkt styku z Internetem – firewall.

Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego. Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego. W trakcie przygotowania i przeprowadzenia szkoleń, a także przygotowania dokumentacji szkoleniowej Wykonawca zobowiązany jest przestrzegać wymagań standardu szkoleniowego i cyfrowego opisanych w dokumencie „Wytyczne dotyczące realizacji zasad równościowych w funduszach unijnych w latach 2021-2027" w brzmieniu obowiązującym na dzień podpisania umowy z wykonawcą. Tekst wytycznych dostępny jest pod adresem https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/fundusze-na-lata-2021-2027/prawo-i-dokumenty/wytyczne/wytyczne-dotyczace-realizacji-zasad-rownosciowych-w-ramach-funduszy-unijnych-na-lata-2021-2027/

6.13. Instalacja i konfiguracja (Platforma sprzętowa) – 100 rbh – wymagania minimalne

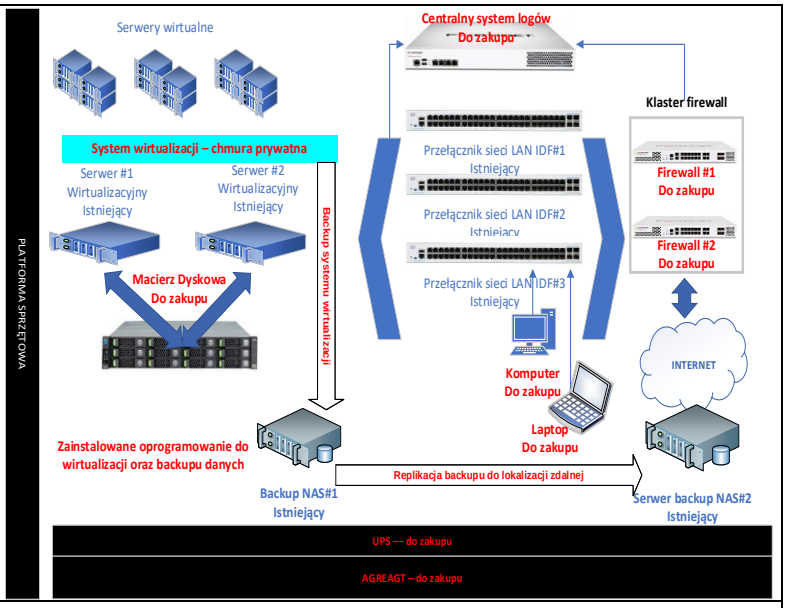
Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.		
1.	**Usługi**	Celem prac jest przygotowanie środowiska teleinformatycznego – platformy sprzętowej, na potrzeby realizacji elementów Zintegrowanego Systemu Informatycznego i cyberbezpieczeństwa, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. Część sprzętowa powinna zostać oparta na rozbudowie systemie wirtualizacji zasobów IT. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. **W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową**. Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym: a) Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia. b) Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności: i. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych. ii. schematy połączeń

		iii. mechanizmy działania głównych elementów sprzętowych: • Firewall/UTM • klaster wirtualizacyjny • system backupu i archiwizacji danych • system serwerowy • system macierzowy iv. iii. mechanizmy działania głównych elementów programowych: • Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa (SIEM/SOAR) • Oprogramowanie do zarzadzania infrastrukturą IT. v. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności vi. sposób odbioru uzgodniony z Zamawiającym vii. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu viii. opis przypadków, w których projekt dopuszcza niedziałanie systemu ix. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia.
2.	**Montaż i fizyczne uruchomienie systemu**	**Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:** 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. 2. Rozbudowa istniejących zasobów sprzętowych. 3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). 10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem:

		a. Stworzenia połączeń sieci LAN pomiędzy przełącznikami. b. Podłączenia urządzeń serwerowo-macierzowych (macierz) do przełączników sieci LAN. c. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1. d. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
3.	**Instalacja i konfiguracja oprogramowania**	1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. 2. Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu. 3. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego). 4. Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych. 5. Instalacja i konfiguracja oprogramowania do monitorowania i analizy cyberbezpieczeństwa (SIEM/SOAR) 6. Instalacja i konfiguracja oprogramowanie do zarzadzania infrastrukturą IT.
4.	**Konfiguracja przełączników/sieci LAN:**	Re/Konfiguracja przełączników w zakresie: a. Przeprowadzenie audytu obecnej topologii oraz konfiguracji. b. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym). c. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy) d. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na urządzeniach firewall. e. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN. f. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster; g. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK). h. Konfiguracja mechanizmów 802.1x na wskazanych portach przełączników w oparciu o certyfikaty komputerów (konfiguracja Centrum Certyfikacji oraz polityk leży po stronie Wykonawcy) z wykorzystaniem istniejącego oprogramowania „NAC” – funkcjonalność Windows Server. i. Testowanie obsługi ruchu sieciowego. j. Testowanie skuteczności zabezpieczeń.
5.	**Konfiguracja elementów bezpieczeństwa sieciowego.**	Konfiguracja/Modernizacja konfiguracji UTM dla nowych urządzeń w zakresie. 1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.

		3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 4. Przygotowanie projektu włączenia dostarczonego urządzenia do sieci LAN urzędu – stworzenie klaster HA. 5. Konfiguracja dostarczonych systemów Firewall: a. Konfiguracja podstawowych parametrów b. Konfiguracja translacji adresów NAT c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp. d. Konfiguracja inspekcji określonych protokołów sieciowych; e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall; f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; g. Testowanie działania bramy 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS: a. Konfiguracja podstawowych parametrów b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań; c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego; d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; e. Testowanie działania ochrony IPS 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. a. Przypisanie adresu IP do zarządzania. b. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3 c. Definicja reguł filtrowania/blokowania d. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny. 8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej. 9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia. 10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN. 11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC 12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności: a. kontrola dostępu - zapora ogniowa klasy Stateful Inspection

		b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS] d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) f. kontrola pasma oraz ruchu [QoS, Traffic shaping] g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P h. Ochrona przed wyciekiem poufnej informacji (DLP) i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL) j. Inspekcja ruchu SSL k. Ochrony przez atakami na stacje klienckie l. Kontrola pasma 13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi. 14. Konfiguracja logowania i raportowania.
6.	**Serwery**	Zamawiający wymaga wykorzystania istniejących serwerów dla klastra niezawodnościowego i wydajnościowego stworzonego na bazie serwerów i dostarczonego oprogramowania do wirtualizacji.
7.	**Serwer backupu - NAS**	W ramach projektu przewiduje się wykorzystanie istniejącego serwera backupu (NAS) na miejsce przechowywanie backupu. Wykonywanie backupu musi być powiązane z procedurą sprawdzania poprawności jego wykonania oraz automatycznym raportowaniem do jednostki administracyjnej. Mechanizm podłączenia 1. Konfiguracja i podłączenie serwera backupu do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 2. Konfiguracja i podłączenie serwera backupu do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 3. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. Logiczny schemat rozbudowywanego systemu backup – stan docelowy.

		
8.	**Macierz dyskowa**	Macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dziedzinowe. Musi zostać podłączona do środowiska wirtualizacyjnego (klaster serwerów). Ilość i wielkość udziałów dyskowych udostępnionych dla serwerów np.: wirtualizacyjnych zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej.
9.	**UPS, Agregat.**	W ramach niniejszego postępowania Zamawiający wymaga podłączenia, skonfigurowania i uruchomienia zaoferowanych urządzeń UPS i Agregat do sieci elektrycznej Urzędu celem zabezpieczenia pomieszczenia serwerowni. Wszystkie koszty z tym związane np.: modernizacji istniejącej instalacji elektrycznej muszą zostać przewidziane i uwzględnione w ofercie Wykonawcy.
10.	**Migracja danych**	Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów. Dane (systemy dziedzinowe) musza zostać przeniesione na nowe zasoby serwerowo-macierzowe. Zakres migracji zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych.
11.	**Serwer SMTP**	Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux. Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z: • Urządzeń sieciowych • Serwerów • Macierzy dyskowej • Systemu zarządzania kopiami zapasowymi • Systemu wirtualizacji serwerów • Aplikacji Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł.

		Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email.
12.	**Instalacja i konfiguracja serwera kopii zapasowych konfiguracji urządzeń sieciowych.**	1. Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.; przełączników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy. 2. Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego). 3. Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie. 4. Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.
13.	**Uruchomienie środowiska wirtualizacyjnego.**	Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie: 1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta. 2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 3. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 4. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach. 5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów. 6. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 7. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 9. Przygotowanie koncepcji wirtualizacji fizycznych maszyn.

		10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym. 11. Konfiguracja klastra wysokiej dostępności: a. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika. b. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn. c. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera. 12. Weryfikacja działania klastra wysokiej dostępności. 13. Migracja istniejącej infrastruktury do środowiska wirtualnego. 14. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową 15. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
14.	**Rekonfiguracja systemu zarządzania kopiami zapasowymi.**	1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na serwerze backupu (wgranie licencji). 2. Aktywacja oraz instalacja niezbędnych licencji. 3. Konfiguracja stacji zarządzającej. 4. Dołączenie klientów do system backupu. 5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania: a. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące; b. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy; c. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu; d. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową; e. musi istnieć możliwość odtworzenia: i. całej wirtualnej maszyny; ii. dysku wirtualnej maszyny; iii. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa); 6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej: a. Nazwę zadania backupu b. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/ c. Długość trwania zadania backupu d. Ilość zapisanych na taśmie danych 7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach: a. Błąd urządzenia b. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi

		c. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi d. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi e. Zdarzenia dotyczące licencji f. Zapełnienia mail-slotu 8. Uruchomienie testowych zadań backupu 9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email 10. Uruchomienie testowych zadań odtworzenia danych 11. Miejscem przechowywania kopii zapasowych jest: a. serwer backupu (NAS). b. na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu.
15.	**Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa**	1. Proces wdrożenia systemu określony powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi oraz zatwierdzonym harmonogramem, umożliwiając efektywne wdrożenie rozwiązania w okresie 3 miesięcy. 2. Proces wdrożeniowy podzielony zostanie na obszary: a. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji). b. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM. c. Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR. 3. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno: a. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki, uzupełnienia ankiety przedwdrożeniowej oraz przygotowania i zatwierdzenia harmonogramu prac). b. Uruchomienie systemu w infrastrukturze zamawiającego, w tym: • konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu, • przygotowanie przez Zamawiającego połączenia zdalnego, • instalację lub import maszyny wirtualnej typu „software appliance”, • aktywację licencji, • wstępną konfigurację, • import/wprowadzenie tabeli adresacji znaczących stref

		bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN). c. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym: • przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu, • uruchomienie reguł wykrywania. d. Prace audytowe, w tym: • pasywną analizę transmisji sieciowej: o o ruch z/do serwerów webowych i aplikacyjnych, o o ruch z/do serwerów baz danych, o o ruch z/do serwerów pocztowych, o o ruch z/do kontrolerów domenowych, o o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP), o o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji. • konsultacje w ramach otrzymanych wyników, • zebranie danych audytowych wymaganych do sporządzenia raportu. e. Analizę podatności, w zakresie: • integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source, • przygotowanie reguł priorytetów i importu krytycznych podatności. f. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać: • zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia, • potencjalne wektory ataków dla wykrytych zagrożeń, • wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków, • rekomendacja zabezpieczeń, • zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń. 4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno: a. Podłączenie (przekierowanie przez Zamawiającego do systemu) źródeł zdarzeń i ich dalszą konfigurację w systemie. Kluczowe źródła zdarzeń obejmują: • zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy), • sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam), • centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR),

		• kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym, • systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA), • system SIEM, • źródła, muszą zostać powiązane z parserami, pozwalającymi na detekcję zgodną z wbudowanymi w system regułami korelacji, b. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą. c. Podłączenie reguł detekcji. d. Podłączenie i konfiguracja mechanizmów UEBA: • integracja z Active Directory, • adaptacja profili użytkowników UBA, • adaptacja profili hostów EBA, • import reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia. 5. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać: a. Import gotowych scenariuszy obsługi. b. Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi. c. Konfigurację mechanizmów powiadamiania. 6. Usługa konsultacji powdrożeniowej, świadczona przez dedykowanego inżyniera w ramach okresu wsparcia musi w szczególności uwzględniać: a. przygotowanie i modyfikację formularzy raportów; b. tworzenie i edycję parserów; c. przygotowywanie nowych reguł bezpieczeństwa; d. modyfikację dostępnych reguł i ich dostrojenie; e. wsparcie w procesie aktualizacji systemu; f. tworzenie i edycję nowych scenariuszy reakcji; g. tworzenie i dostosowanie dashboardów danych. 7. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu. Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 5 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.

16.	**Oprogramowanie do zarzadzania infrastrukturą IT.**	System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem. Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności. Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności.
17.	**Testowanie i modyfikacja parametrów infrastruktury sieciowej.**	1. Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego. 2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. 3. Testowanie mechanizmów replikacji danych. 4. Testowanie dostępu publicznego do zasobów. 5. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu 6. Testowanie autoryzowanego dostępu do wewnętrznych zasobów. 7. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach
18.	**Asysty stanowiskowe**	Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia. Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego. Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego.
19.	**Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.**	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą. **Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.** W tym czasie przedstawiciel Wykonawcy: • zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. • dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności: a) zastosowanej technologii serwerów b) zastosowanej technologii pamięci masowej c) wirtualizacji d) systemu backupu

		e) zastosowanych rozwiązań aplikacyjnych Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania.
20.	**Opracowanie dokumentacji powykonawczej**	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu. 1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów. 2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację). 3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały. 5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.

7. Szczegółowy opis pozycji – część 2.

7.1. Oprogramowanie dziedzinowe – licencja szt. 1 – wymagania minimalne

Wymagania funkcjonalne modułu obsługa podatku rolnego, leśnego i od nieruchomości.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł musi zapewnić ewidencjonowanie kart podatkowych z uwzględnieniem podziału na sołectwa/obręby podatkowe i stosować odpowiednią numerację uwzględniającą ten podział.
2. Moduł musi rozdzielać ewidencję osób fizycznych i prawnych.
3. Ewidencja kart podatkowych dla osób fizycznych musi być wspólna dla wszystkich rodzajów podatków.
4. Użytkownik musi mieć możliwość wyboru grup kart w zakresie sposobu opodatkowania (podatek rolny, leśny, od nieruchomości, łączne zobowiązanie), sołectwa lub obrębu podatkowego, ulicy zarówno dla osób fizycznych jak i prawnych.
5. Moduł musi umożliwiać łączenie kart podatkowych i scalanie ich danych automatycznie zarówno przez wywołanie funkcji scalającej jak i scalenie wszystkich pozycji oznaczonych jako powiązane np. przy opcji zamknięcia roku podatkowego lub wywołaniu odpowiedniego polecenia przez administratora systemu. Karta po scaleniu musi zawierać przedmioty opodatkowania znajdujące się na wszystkich powiązanych kartach. Użytkownik określa nadrzędną kartę do której będą przeniesione dane z kart podrzędnych.
6. Moduł musi umożliwiać prowadzenie ewidencji danych personalnych podatników w szerokim zakresie z możliwością przeglądania historii dokonywanych zmian minimum w zakresie podstawowych danych personalnych oraz adresu podatnika.
7. Moduł musi umożliwiać wprowadzanie wielu adresów związanych z danym podatnikiem (minimum adres zamieszkania i korespondencyjny).
8. Moduł powinien umożliwić prowadzenie ewidencji działek i musi uwzględniać możliwość wprowadzenia przy nich informacji o udziałach z uwzględnieniem historii zmian. W zakresie ewidencji działek powinna być też możliwość powiązania wprowadzonych gruntów z wybraną działką.

9. Moduł musi posiadać możliwość wprowadzania zarówno ulg i zwolnień ustawowych jak i wprowadzonych uchwałą Rady Gminy w odniesieniu do poszczególnych rodzajów podatków
10. Moduł musi uwzględniać możliwość naliczania podatku rolnego wg. hektarów fizycznych i przeliczeniowych. Zmiana sposobu opodatkowania w roku podatkowym nie może wymuszać założenia nowej karty, a jedynie wprowadzenia daty od której ma nastąpić zmiana sposobu jego naliczania.
11. Moduł w naliczaniu wymiaru podatku musi wyliczyć odpowiednie kwoty z uwzględnieniem podziału na poszczególne rodzaje zobowiązań (rolny, leśny i od nieruchomości) oraz raty podatku z uwzględnieniem obowiązujących terminów płatności oraz specyfiki naliczania podatków w zakresie osób fizycznych i prawnych.
12. Naliczanie wymiaru powinno być dokonywane w trybie zbiorczym dla całości podatników lub wybraneej grupy podatników sołectwo/obręb podatkowy.
13. Moduł musi umożliwiać naliczanie zmian w wysokości podatku i wydawanie stosownych decyzji zarówno w odniesieniu do bieżącego roku jak i lat ubiegłych
14. Moduł musi umożliwiać drukowanie odpowiednich decyzji z uwzględnieniem wydruków zbiorczych dla grup podatników oraz wydruk dla pojedynczych kart.
15. Moduł musi umożliwiać generowanie decyzji elektronicznych i wysyłanie ich za pośrednictwem modułu integrującego do systemu (EOD). Rejestracja w systemie EOD musi uwzględniać rejestracją sprawy zgodnie z konfiguracją systemu w zakresie jednolitego rzeczowego wykazu, kartoteki kontrahentów, dat i typów.
16. Moduł musi umożliwiać wczytywanie do systemu deklaracji i załączników złożonych przez podatnika za pomocą platformy ePUAP.
17. Moduł powinien umożliwić wydruk informacji podatkowych (Ir-1, In-1, Il-1 wraz z załącznikami) na podstawie danych zaewidencjonowanych w systemie.
18. Moduł powinien umożliwić wydruk deklaracji podatkowych (DR-1, DN-1, DL-1 wraz z załącznikami) na podstawie danych zaewidencjonowanych w systemie.
19. Moduł powinien umożliwić obsługę elektronicznych zawiadomień o zmianach w danych ewidencyjnych z Ewidencji gruntów i budynków.
20. Moduł musi posiadać funkcjonalność modyfikacji standardowych wzorów wydruków oraz możliwość wprowadzania nowych wzorów. Musi także uwzględniać możliwość tworzenia wydruków w formacie RTF z uwzględnieniem automatycznego wypełniania wydruku danymi z programu. System musi umożliwiać generowanie wydruków na podstawie tych wzorców i zapisywanie ich w systemie obiegu dokumentów EOD w profilu użytkownika z uwzględnieniem typów dokumentów w nim zdefiniowanych. W szczególności dotyczy to wydruku zaświadczeń wg wzorców opracowanych przez użytkownika.
21. Moduł musi umożliwiać drukowanie zaświadczeń do pliku PDF i wysyłanie ich za pośrednictwem modułu integrującego i systemu EOD.
22. Moduł musi umożliwić wydawanie zaświadczeń z wielu kart na jednym wydruku. Użytkownik musi mieć możliwość oznaczenia kart, z których chce wydać zaświadczenie.
23. Moduł musi posiadać rejestr wydanych zaświadczeń.
24. Moduł musi umożliwiać wydruk blankietów dowodów wpłat, potwierdzeń odbioru decyzji z możliwością drukowania w/w dokumentów łącznie z decyzjami wymiarowymi. Moduł musi umożliwiać drukowanie w/w dokumentów do pliku PDF i wysyłanie ich za pośrednictwem modułu integrującego i systemu EOD.
25. Moduł musi umożliwiać oznaczanie wydruków kodem kreskowym identyfikującym daną kartę podatkową oraz kodów kreskowych identyfikujących poszczególne raty zobowiązania w celu integracji z systemami bankowymi w zakresie obsługi indywidualnych rachunków bankowych dla płatności masowych.
26. Wszystkie dokonane wydruki decyzji wymiarowych i zmieniających wymiar muszą być zapisywane do bazy danych i gromadzone na karcie podatnika. W każdym momencie użytkownik może podglądnąć i wydrukować na nowo taką decyzją w niezmienionym formacie.
27. Moduł musi posiadać możliwość generowania wydruków wybranych pism (decyzji) do formatu RTF z możliwością ich edycji i zapisu do karty podatnika i wysyłania ich za pośrednictwem modułu integrującego i systemu EOD.

28. Moduł musi umożliwiać prowadzenie (wydruk) rejestru wymiarowego oraz rejestru przypisów i odpisów. Wydruki te powinny mieć możliwość zapisu duplikatu rejestru wymiarowego do pliku PDF oraz zapisanie go za pośrednictwem modułu integrującego w systemie EOD.
29. Moduł musi posiadać możliwość wielopłaszczyznowej analizy wprowadzanych danych i możliwość ich raportowania w postaci wydruków. W szczególności wymagane będą zestawienia z uwzględnieniem podziału na sołectwa/okręgi podatkowe uwzględniające wysokość poszczególnych podatków, szczegółową analizę ulg i zwolnień oraz skutków obniżenia stawek w podatku rolnym i od nieruchomości. Zestawienia te muszą dawać też możliwość uzyskania informacji o łącznej ilości przedmiotów opodatkowania oraz o wysokości podstawy ich wymiaru.
30. Moduł musi umożliwiać przegląd historii właścicieli nieruchomości.
31. Moduł musi uwzględniać możliwość wydruku indywidualnych numerów rachunków bankowych na które będą dokonywać wpłaty podatnicy. Moduł musi uwzględniać możliwość dostosowania w/w rozwiązania do wymogów bankowych płatności masowych.
32. Moduł musi dawać możliwość wydruku odpowiednich danych w postaci kodu kreskowego na blankiecie dowodu wpłaty z możliwością wprowadzenia w nim identyfikacji płatnika, kwoty wpłaty, identyfikacji zobowiązania.
33. Moduł musi współpracować z systemem eNależności oraz aplikacją mobilną za pośrednictwem serwisu komunikacyjnego w zakresie informacji dotyczących zobowiązań, danych ewidencyjnych kartoteki podatnika oraz podglądu dokumentów (decyzji, zaświadczeń) wystawianych przez system.
34. Komunikacja z systemem (EOD – elektroniczny obieg dokumentów) odbywa się za pośrednictwem modułów szyny danych i brokera komunikacyjnego z wykorzystaniem usługi web service.
35. System musi zapewnić obsługę e-usług w zakresie niezbędnym do ich realizacji.

Wymagania funkcjonalne modułu obsługa podatku od środków transportu

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł musi posiadać możliwość wprowadzania danych pojazdów i dokonywania zmian/poprawek (zgłoszenie sprzedaży, zmiana właściciela, zmiana parametrów technicznych itp.) w zakresie umożliwiającym prawidłowe naliczenie kwot podatku.
2. Moduł musi umożliwiać obsługę słowników takich jak: słownik stawek podatków na poszczególne lata, słownik terminów płatności, rodzajów i marki pojazdu).
3. Moduł musi umożliwiać wyszukiwanie podatnika po minimum wymienionych kryteriach: nazwa/nazwisko, numer rejestracyjny pojazdu, adresu zamieszkania/siedziby, numer karty kontowej podatnika.
4. Moduł musi umożliwiać rejestrację decyzji uznaniowych (np. umorzenie odsetek lub ich części, odroczenie terminów płatności, rozłożenie płatności na raty).
5. Moduł musi umożliwiać tworzenie raportów i zestawień w minimalnym zakresie zdefiniowanym poniżej:
    a. Zestawienie podatników z naliczonym wymiarem.
    b. Zestawienie podatników bez naliczonego wymiaru.
    c. Zestawienie przypisów i odpisów.
    d. Rejestr pism.
    e. Rejestr decyzji uznaniowych.
    f. Statystyka właścicieli pojazdów.
    g. Statystyka osób, które złożyły, bądź nie złożyły deklaracji za dany rok podatkowy.
6. Moduł musi umożliwiać rejestrowanie elektronicznych deklaracji DT-1 złożonych przez podatnika za pośrednictwem platformy ePUAP. Pobieranie i wczytywanie do systemu deklaracji i załączników złożonych przez podatnika za pomocą platformy ePUAP dokonywane ma być bezpośrednio z systemu EOD za pośrednictwem mechanizmów integrujących z uwzględnieniem odpowiednich typów dokumentów zdefiniowanych w systemie obiegu dokumentów.
7. Moduł musi posiadać kreator wydruku deklaracji podatkowych (DT – 1) wraz z załącznikami na podstawie danych zaewidencjonowanych w systemie.

8. Moduł musi umożliwiać weryfikację błędnie wprowadzonych deklaracji i odesłanie zwrotnej elektronicznej informacji za pomocą systemu EOD do podatnika na jego konto na platformie ePUAP lub w systemie eDoreczeń.
9. Moduł musi współpracować z systemem eNależności oraz aplikacją mobilną za pośrednictwem serwisu komunikacyjnego w zakresie informacji dotyczących zobowiązań, danych ewidencyjnych pojazdów oraz podglądu dokumentów wystawianych przez system.
10. System musi zapewnić obsługę e-usług w zakresie niezbędnym do ich realizacji.

Wymagania funkcjonalne modułu obsługa opłat za gospodarowanie odpadami komunalnymi

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł do obsługi opłat za gospodarowanie odpadami komunalnymi musi umożliwiać prowadzenie szczegółowej ewidencji płatników.
2. Moduł musi dokonywać okresowych rozliczeń należności z tytułu wywozu nieczystości.
3. Moduł musi posiadać wszystkie funkcje związane z naliczaniem opłat, podziałem na raty i przypisaniem należności w systemie module księgowym.
4. Moduł musi mieć możliwość edycji formy i treści informacji o wysokości opłaty, decyzji ustalającej wysokość opłaty wraz z potwierdzeniami odbioru oraz możliwość tworzenia innych dowolnych dokumentów.
5. Moduł musi mieć możliwość wydruku informacji o wysokości opłaty lub decyzji ustalającej jej wysokość oraz innych definiowalnych pism dla wybranych osób lub miejscowości i automatyczne przekazanie (rejestracja jako pismo) ich do systemu EOD za pośrednictwem modułu integrującego.
6. Moduł musi umożliwiać wczytywanie do systemu deklaracji i załączników złożonych przez podatnika za pomocą platformy ePUAP pobranych z systemu EOD za pośrednictwem modułów komunikacyjnych z uwzględnieniem typów dokumentów funkcjonujących w systemie obiegu dokumentów. Dane z deklaracji elektronicznej powinny zostać automatycznie przepisane do systemu dziedzinowego. System powinien umożliwić wprowadzanie zarówno nowych deklaracji jak i rejestracje korekty zeznania.
7. Moduł musi zapewniać wyszukiwanie podatników wg nazwiska lub numeru karty oraz adresu podatnika i posesji z której odbierane są odpady.
8. Moduł musi generować wydruki na drukarkę, na ekran lub do pliku PDF.
9. Moduł musi umożliwiać tworzenie i przeglądanie danych archiwalnych.
10. Moduł musi umożliwić drukowanie i obsługę kodów kreskowych w oparciu o druk termotransferowy umożliwiających znakowanie odpadów i otrzymanie zwrotnej informacji dotyczącej daty dokonania wywozu, numeru kodu kreskowego, rodzaju odpadu oraz współrzędnych GPS miejsca odbioru odpadu.
11. Moduł musi współpracować z przenośnymi skanerami kodów kreskowych obsługującymi lokalizację odczytu kodu kreskowego za pośrednictwem współrzędnych GPS.
12. System powinien zapewnić wizualizację miejsca odbioru odpadu na podstawie współrzędnych GPS uzyskanych w trakcie odczytu kodów kreskowych.
13. Moduł musi zapewnić integracje z systemami bankowymi w zakresie płatności masowych.
14. Moduł musi współpracować z systemem eNależności oraz aplikacją mobilną za pośrednictwem serwisu komunikacyjnego w zakresie informacji dotyczących zobowiązań, danych ewidencyjnych kartoteki podatnika.
15. Komunikacja z systemem EOD odbywa się za pośrednictwem modułów szyny danych i brokera komunikacyjnego z wykorzystaniem udostępnionej usługi.
16. System musi zapewnić obsługę e-usług w zakresie niezbędnym do ich realizacji.

Wymagania funkcjonalne modułu ewidencja zbiorników bezodpływowych

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Funkcjonalności systemu muszą być dostępne wyłącznie dla zalogowanych użytkowników.
2. System musi umożliwiać ewidencjonowanie zbiorników bezodpływowych z uwzględnieniem wprowadzenia danych takich jak:
    - Rodzaj zbiornika
    - Pojemność
    - Data budowy oraz ewentualnej likwidacji

- Technologia wykonania
- Rodzaj nieczystości
- Częstotliwość opróżniania
- Data wprowadzenia do ewidencji
- Opis

3. System musi umożliwiać wprowadzenie dowolnej ilości zbiorników przypisanych do jednej posesji.
4. System musi pozwalać na przypisywanie do zbiornika umów zawartych z firmą wywożącą.
5. System musi umożliwiać wybieranie danych z wcześniej wypełnionych słowników takich jak:
    - Rodzaj zbiornika
    - Firma wywożąca nieczystości
    - Częstotliwość opróżniania zbiornika
    - Technologia wykonania zbiornika
    - Rodzaj nieczystości
6. System musi umożliwiać wprowadzenie do umowy:
    - Dane nieruchomości – miejscowość, ulica, nr domu i lokalu, nr działki
    - Rodzaj zbiornika
    - Dane umowy – nr umowy, data zawarcia umowy, okres umowy, osoba zawierająca
    - Dane firmy wywożącej
    - Uwagi
7. System musi pozwalać na przypisywanie do zbiornika listy wywozów zawierających dane takie jak:
    - Ilość wywożonych nieczystości
    - Data wywozu
    - Firma wywożąca
    - Uwagi
8. System musi umożliwiać wprowadzanie kontroli zbiorników bezodpływowych wraz z następującymi danymi:
    - Dane osoby kontrolowanej – nazwisko, imię
    - Dane posesji kontrolowanej – miejscowość, ulica, ilość osób zameldowanych, zamieszkałych i zadeklarowanych, nr działki, nr domu, nr lokalu
    - Dane zbiornika – rodzaj, pojemność, data budowy, data likwidacji, technologia wykonania, rodzaj nieczystości
    - Dane umowy – nr umowy, data zawarcia, firma wywożąca, okres umowy, osoba zawierająca
    - Dane kontroli – miejsce kontroli oznaczenie czy kontrola odbyła się w terenie czy w Urzędzie, data kontroli, nr kontroli, osoba kontrolowana, ustalenia, uwagi, zalecenia po kontroli oraz możliwość oznaczenia czy przedstawiono faktury za wywóz nieczystości
    - Możliwość wprowadzenia danych przynajmniej trzech osób przeprowadzających kontrolę – imię, nazwisko oraz stanowisko
    - Możliwość wgrania załączników do kontroli z dysku
9. System musi umożliwiać zatwierdzanie kontroli.
10. System musi umożliwiać wprowadzenie zużycia wody w danej posesji z danymi takimi jak:
    - Data faktury
    - Okres zużycia
    - Ilość
    - Uwagi
11. System musi umożliwiać wprowadzanie adnotacji zawierających datę wprowadzenia oraz treść.
12. System musi umożliwiać generowanie wydruku listy wywozów dla zbiornika wprowadzonego w danej posesji.
13. System musi umożliwiać generowanie wydruku protokołu kontroli danego zbiornika.
14. System musi umożliwiać generowanie wydruku zużycia wody dla danej posesji.
15. System musi umożliwiać generowanie wydruku listy posesji.

16. System musi pozwalać na wyświetlanie rejestru zbiorników oraz filtrowanie go według kryteriów:
    - Lokalizacja – obręb, miejscowość, ulica, nr domu, nr lokalu
    - Dane zbiornika – rodzaj, pojemność od do, technologia wykonania, rodzaj nieczystości, osoba, data wprowadzenia do systemu, data wybudowania
    - Dane umowy – nr umowy, firma wywożąca, data zawarcia umowy, okres umowy
    - Lista wywozów – wywóz w konkretnym terminie, ostatni wywóz
    - Lista kontroli – kontrola przeprowadzona w okresie
17. System musi pozwalać na sortowanie rejestru zbiorników według kryteriów:
    - Dane płatnika
    - Adres posesji
    - Obręb opłat następnie adres posesji
    - Obręb opłat następnie płatnik
    - Rodzaj zbiornika
18. System musi umożliwiać generowanie wydruku rejestru zbiorników według posesji oraz według zbiornika.
19. System musi pozwalać na wyświetlanie zestawienia umów oraz filtrowanie ich według kryteriów takich jak:
    - Dane umowy – nr umowy, firma wywożąca, data zawarcia umowy, okres umowy, rodzaj zbiornika
    - Dane adresowe – miejscowość, ulica, nr domu, nr lokalu
20. System musi pozwalać na wyświetlanie rejestru kontroli oraz filtrowanie go według kryteriów
    - Dane adresowe – osoba, miejscowość, ulica, nr domu, nr lokalu
    - Dane zbiornika – rodzaj zbiornika, pojemność, technologia wykonania, rodzaj nieczystości
    - Dane kontroli – data kontroli, oznaczenie czy kontrola została przeprowadzona w terenie czy w urzędzie
21. System musi umożliwiać zapisanie danych z rejestru zbiorników, zestawienia umów, rejestru kontroli do pliku w formacie .csv
22. System musi umożliwiać generowanie sprawozdań z gospodarowania nieczystościami ciekłymi.

Wymagania funkcjonalne modułu księgowości podatkowej

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł w swoim zakresie musi obsługiwać w wydzielonych ewidencjach wiele kontekstów (rodzajów) opłat i podatków z możliwością ich parametryzacji.
2. W zakresie konfiguracji kontekstu wymagane jest min. Określenie jego nazwy, klasyfikacji budżetowej, sposobu naliczania odsetek, sposobu nadawania indywidualnych numerów bankowych oraz zasad przekazywania danych zbiorczych do systemu finansowo-księgowego.
3. Konfiguracja kontekstów powinna także uwzględniać wizualizację danych w portalu eBOM.
4. Ewidencja kart kontowych zgodna z ustawą o rachunkowości oraz ordynacją podatkową z uwzględnieniem podziału na sołectwa/okręgi podatkowe lub obręby.
5. Poszczególnym kartom opłat z wymiaru odpowiadają konta w systemie księgowym.
6. Moduł musi umożliwiać przeglądanie karty kontowej podatnika oraz zawartych na niej wszelkich zapisów księgowych wraz z wydrukiem takiej karty i możliwością jej przekazania do systemu EOD za pośrednictwem modułu integrującego.
7. Moduł musi umożliwiać automatyczne rejestrowanie wpływów zaksięgowanych w module kasowym na konta podatników.
8. Moduł musi umożliwiać rozksięgowanie wpłat z wyciągu bankowego z możliwością:
    a. zarachowanie od najstarszej zaległości,
    b. zarachowanie na wskazaną należność,
    c. automatyczne wyliczenie i pobranie odsetek.
9. Moduł musi umożliwiać przeksięgowanie nadpłat na inną należność podatkową, na inny rodzaj podatku lub zwrot nadpłaty podatnikowi.
10. Moduł musi umożliwiać anulowanie upomnień i tytułów wykonawczych.

11. Moduł musi umożliwiać uzyskanie informacji o zaległościach w rozbiciu na należność główną, odsetki na wybrany dzień.
12. Moduł musi umożliwiać tworzenie wydruków, w szczególności:
    a. Zestawienie bilansowe
    b. Zestawienie zawierające dane do RB-27S
    c. Zestawienie syntetyczne zawierające podsumowanie okresu
    d. Zestawienie syntetyczne zawierające salda wpływów
13. Zapisy wszystkich operacji księgowych na odpowiednich kontach podatników dokonywane są w systemie dwustronnym z uwzględnieniem księgowań na kontach przeciwstawnych. Zapisy te dokonywane są po odpowiednich stronach WINIEN, MA.
14. Zapisy księgowań na odpowiednich paragrafach budżetowych. Wizualizacja danych na koncie w układzie budżetowym
15. Informacja o aktualnym stanie zadłużenia na koncie oraz o wysokości należnych odsetek na dany dzień.
16. Zapisy księgowe grupowane są w obrębie odpowiedniego typu księgowania (np. rejestr wymiarowy, raport kasowy, wyciąg bankowy, itp.). Wszystkie te grupy mają możliwość zbiorczego zaksięgowania i zablokowania możliwości dokonania zmian w obrębie tej pozycji.
17. Możliwość wprowadzania umorzeń należności głównej i odsetek.
18. Możliwość wprowadzania rozłożenia należności na raty oraz przesunięcia terminów płatności.
19. Księgowanie wpłat z uwzględnieniem automatycznego księgowania na najstarsze należności i automatyczne dzielenie kwoty wpłaty na należność główną, odsetki koszty egzekucji.
20. Wydruki postanowień o zarachowaniu wpłaty.
21. Możliwość wydruków upomnień i tytułów wykonawczych oraz prowadzenie ich ewidencji. Przy generowaniu zbiorowym upomnień użytkownik może określić jakie należności chce umieścić na upomnieniu oraz określić minimalną kwotę od której będą wystawiane upomnienia. Wzory upomnienia i tytułu wykonawczego mogą być modyfikowane przez użytkownika.
22. W zakresie tytułów wykonawczych moduł musi wspierać pełen proces od utworzenia tytułu poprzez jego walidację i podpisanie go certyfikatem kwalifikowanym oraz przekazanie do urzędu skarbowego za pośrednictwem systemu eTW. Proces generowania, podpisywania oraz przekazywania tytułów powinien być w całości realizowany w obrębie systemu. Użytkownik powinien mieć możliwość weryfikacji poprawności przesłania tytułu do eTW (możliwość pobrania UPO).
23. Wydruk sprawozdanie RB-27S oraz RBN na podstawie zapisów dokonanych na poszczególnych kontach.
24. Wielopłaszczyznowa analiza wprowadzanych danych i możliwość ich raportowania w postaci wydruków
25. Zbiorcze przeksięgowania nadpłat początkowych na należności bieżące z uwzględnieniem odpowiedniego zapisu na paragrafach budżetowych.
26. Możliwość zablokowania zapisów księgowych do wybranej daty w przypadku uzgodnienia danego okresu obliczeniowego (zbiorcze zaksięgowanie dokumentów).
27. Wydruk dziennika obrotów.
28. Automatyczne księgowanie wpłat na podstawie elektronicznego wyciągu bankowego przy uruchomieniu indywidualnych rachunków bankowych w systemie wymiarowym.
29. Współpraca z czytnikiem kodów kreskowych w zakresie identyfikacji podatnika i automatycznego wprowadzania dowodów wpłat sygnowanych kodami kreskowymi (np. przy wydruku blankietów wpłat dla inkasentów).
30. Integracja z systemem finansowo-księgowym w zakresie przesyłania noty księgowej do systemu finansowo-księgowego z zastosowaniem formatu XML lub inną metodą.
31. Moduł musi umożliwiać drukowanie dokumentów do pliku PDF i wysyłanie ich za pośrednictwem modułu integrującego do systemu EOD.
32. Moduł musi współpracować z systemem eNależności oraz aplikacją mobilną za pośrednictwem serwisu komunikacyjnego w zakresie informacji dotyczących wysokości należnych kwot zobowiązań uwzględniając w szczególności wysokość kwoty należności głównej, należnych odsetek, terminów płatności, dokonanych wpłat.
33. Komunikacja z systemem EOD odbywa się za pośrednictwem specjalistycznych modułów szyny danych i brokera komunikacyjnego z wykorzystaniem udostępnionych usług komunikacyjnych.

34. System musi zapewnić obsługę e-usług w zakresie niezbędnym do ich realizacji.
35. System musi umożliwiać wysyłanie przypomnień o zaległościach z uwzględnieniem podziału na raty w podatkach i opłatach (podatki rolny, leśny, nieruchomość, transportowe) śmieci, woda, kanalizacja) i przesyłać je do podatników zgodnie z wymogami określonymi dla platformy eBOM w zakresie wymogów specyfikowanych w punkcie „Komunikaty, powiadomienia i ogłoszenia, aktualności"

Wymagania funkcjonalne modułu obsługa ewidencji zwrotu podatku akcyzowego zawartego w paliwie.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł musi w pełni realizować wymogi ustawy z dnia 10 marca 2006 o zwrocie podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej poprzez następujące funkcje:
    a. Ewidencja wniosków o zwrot podatku akcyzowego wraz z załącznikami.
    b. Kartoteka wniosków i decyzji.
2. Moduł musi umożliwiać rejestrację wniosku poprzez wczytanie e-formularza wniosku przesłanego z platformy ePUAP w formacie XML. Po wczytaniu wniosku moduł musi wygenerować dokument potwierdzający prawidłowość i kompletność lub stosowne braki do jego uzupełnienia. Informacja ta poprzez moduł integrujący musi zostać przekazana do system EOD, a następnie po podpisaniu podpisem elektronicznym referenta wysłana do wnioskodawcy.
3. Wydanie (wydruk) decyzji musi odbywać się przez wybranie z listy dostępnych wzorów pism, decyzji z możliwością jego rejestracji w repozytorium dokumentów systemu EOD za pośrednictwem modułów komunikacyjnych.
4. Moduł musi zapewniać obsługę dwóch typów list: KASA lub BANK. Wnioskodawca podczas składania wniosku, decyduje o formie wypłaty: gotówka lub rachunek bankowy, jeżeli wybierze gotówkę, wówczas naliczone pieniądze do zwrotu mogą być umieszczone wyłącznie na liście typu KASA, z drugiej strony, jeżeli wskaże rachunek bankowy, wówczas naliczone pieniądze trafią na listę wypłat typu BANK.
5. Sprawozdawczość modułu musi umożliwiać generowanie wydruków: Wniosek o dotacje, Okresowe sprawozdanie, Roczne sprawozdanie, Okresowe rozliczenie, Roczne rozliczenie. Moduł musi umożliwiać drukowanie duplikatów ww. dokumentów do pliku PDF i ich zapis w systemie EOD za pośrednictwem modułu integrującego.
6. Moduł musi zapewniać kontrole powierzchni gruntów na podstawie ewidencji podatkowej. Ze względu na to, iż dane z wniosków należy porównać z ewidencją gruntów musi istnieć możliwość weryfikacji danych o gruntach z modułu podatkowego lub innego rejestru zawierającego dane EGIB.

Wymagania funkcjonalne modułu finansowo-ksiegowego.
System finansowo – księgowy powinien posiadać szereg podmodułów odpowiadających za realizacje następujących obszarów: finanse i budżet, rejestry VAT, rejestr umów, obsługa wydatków .

Finanse i budżet:

1. Moduł musi spełniać wymagania określone przepisami ustawy o finansach publicznych, o rachunkowości, o wydatkach strukturalnych, o sprawozdawczości budżetowej.
2. Moduł musi posiadać możliwość kontekstowego trybu pracy tj. definiowalna struktura jednostek organizacyjnych oraz dzienników dostosowana do zakresu obowiązków pracowników.
3. Moduł musi posiadać możliwość definiowania dostępu do poszczególnych opcji menu oraz elementów struktury organizacyjnej (jednostka/dziennik), tak aby odpowiadało to zakresowi obowiązków (podgląd/edycja /administrowanie).
4. Moduł musi mieć możliwość wglądu w przetwarzane dane w sposób wynikający z nadanych uprawnień tj. dostęp do informacji wybranego dziennika lub księgi głównej będącej agregacją zapisów wszystkich zdefiniowanych dzienników.
5. Moduł musi pozwalać na prowadzenie ewidencji zaangażowania środków budżetowych w poszczególnych paragrafach klasyfikacji budżetowej na poziomie każdej jednostki organizacyjnej, jak i całego budżetu.

6. Moduł musi posiadać warstwę prezentacyjną pozwalającą na swobodne przeglądanie stanu wykonania budżetu z uwzględnieniem wartości:
    a. planu, realizacji, % realizacji (stosunek plan/realizacja), różnicy plan – realizacja,
    b. kosztów, % kosztów (stosunek plan/koszty),
    c. zaangażowania środków RB, różnicy plan – zaangażowanie RB , % zaangażowania RB (stosunek plan/zaangażowanie RB) ,
    d. zaangażowania środków LN
7. Moduł powinien pozwalać na prowadzenie analiz wg. kryteriów:
    a. dział, rozdział, dział/rozdział/ paragraf, dział/rozdział/paragraf/analityka,
    b. wydział, jednostka organizacyjna, zadanie,
    c. dział/rozdział/paragraf/analityka – zadanie,
    d. dziennik,
    e. okres rozliczeniowy.
8. Moduł musi pozwalać na wprowadzanie i księgowanie jednostkowych sprawozdań z wykonania wydatków oraz dochodów budżetowych, (import plików, bezpośrednie pobranie z portalu sprawozdawczości za pomocą serwisów komunikacyjnych).
9. Moduł musi mieć możliwość definiowania oraz sporządzania zestawień wynikowych takich jak:
    a. zestawienie zmian funduszu,
    b. rachunek zysków i strat,
    c. bilans jednostki,
    d. bilans skonsolidowany.
10. Moduł musi realizować obsługę sprawozdań budżetowych w zakresie:
    a. dochodów budżetowych,
    b. wydatków budżetowych
    c. nadwyżki lub deficytu budżetowego,
    d. stanu zobowiązań i należności,
11. Moduł musi pozwalać na przeglądanie stanów i obrotów kont, oraz ich wydruk w formie kont syntetycznych i analitycznych w formacie A4.
12. Moduł musi posiadać możliwość importu uchwał budżetowych z systemu planowania budżetu.
13. Moduł musi pozwalać na generowanie zestawień i ich wydruk w przekroju jednostek organizacyjnych, klasyfikacji budżetowej oraz zadań, zapisywanie tych zestawień do formatu PDF i wysyłanie w formie elektronicznej do jednostek poprzez system EOD.
14. Moduł musi pozwalać na generowanie raportów sprawozdawczych dla RIO (Rb-27S, Rb-27zz, Rb-28S, Rb-30S, Rb-34S, Rb-50,Rb-Nds, Rb-Z, Rb-N, RB-ZN, RB-UZ, RB-UN, RB-PDP) z możliwością ich eksportu do programu BeSTi@.
15. Moduł musi generować w postaci elektronicznej sprawozdania w formacie wymaganym przez RIO i eksportować dane do wymaganego przez RIO systemu sprawozdawczości budżetowej (obecnie system Besti@ i obowiązujące prawnie systemy sprawozdawcze).
16. Funkcjonalność sprawozdawczości budżetowej powinna zwierać również możliwość:
    - agregacji sprawozdań jednostkowych do sprawozdania zbiorczego,
    - importu sprawozdań z formatu innego niż Besti@ np. xls,
    - tworzenia sprawozdań różnicowych – wykonanie budżetu za miesiąc, - generowanie dokumentów księgowych na podstawie danych sprawozdań różnicowych (wykonanie budżetu za miesiąc).
17. Moduł musi posiadać moduł kontroli informujący o przekroczeniach zaplanowanego budżetu w zakresie klasyfikacji budżetowej, zadań oraz umów.
    Rodzaje przekroczeń które muszą podlegać analizie:
    - plan na paragrafie / wydatki;
    - plan na paragrafie / koszty;
    - plan na paragrafie / zaangażowanie RB;
    - wydatki / zaangażowanie RB;
    - plan na zadaniu / wydatki;
    - plan na zadaniu / koszty;
    - plan na zadaniu / zaangażowanie RB;
18. Moduł musi umożliwiać przygotowanie zestawień i ich wydruk:
    a. o przekroczeniu wykonania wydatków ponad plan,

b. o zobowiązaniach przekraczających plany wydatków,
c. o zaangażowaniu przekraczającym plany wydatków,
d. planu oraz wykonania kosztów i wydatków wg klasyfikacji budżetowej,
e. o wydatkach przekraczających zaangażowanie wynikające z umowy,
f. o zobowiązaniach, należnościach wymagalnych.

19. Moduł musi pozwalać na wprowadzanie bilansu otwarcia (generowanie B.O. automatycznie) z możliwością:
    a. ręcznego i automatycznego wprowadzania,
    b. tworzenia roboczego zbioru BO, który może być modyfikowany przed ostatecznym zamknięciem lub możliwość innego korygowania BO,
    c. generowania łącznego BO, BZ dla kilku jednostek organizacyjnych,
    d. generowania i drukowania zestawienia BO, BZ w formacie A4.
    e. Zbiory BO, BZ (salda dwustronne).
20. Moduł musi zapewniać zamknięcie roku z możliwością zachowania na koniec zamykanego roku sald wszystkich kont analitycznych i jednocześnie uzyskania zerowych sald wybranych kont syntetycznych - salda dwustronne.
21. Moduł musi umożliwiać rejestrację operacji gospodarczych w dziennikach z możliwością:
    a. storna czarnego i czerwonego,
    b. generowania i drukowania dziennika w formacie A4
    c. wprowadzenia dokumentu księgowego i jego zapłaty w rozbiciu na źródła finansowania a zarazem uzyskania łącznej kwoty na danym koncie analitycznym.
22. Prowadzenie planu kont z możliwością:
    a. korekty definicji konta,
    b. usuwania konta z planu,
    c. blokady konta,
    d. generowania i drukowania planu kont w formacie A4
    e. tworzenia o dowolnej głębokości analityki, z wykorzystaniem zarówno cyfr jak i liter przy jego budowie.
23. Moduł musi umożliwiać automatyczne i ciągłe numerowanie dowodów księgowych.
24. Moduł musi umożliwiać tworzenie procedur automatycznego dokonywania przeksięgowywań rocznych i miesięcznych, zgodnie z ustawą o rachunkowości (grupy kont 1,2,4,5,7,8 oraz przeksięgowań i wyksięgowań obowiązujących dla rozpoczęcia roku (konta grupy 8 i pozabilansowe wydatków strukturalnych).
25. Moduł musi zapewniać możliwość rejestracji różnych typów dokumentów dochodowych, przychodowych, rozchodowych i wydatkowych, w tym m.in.:
    a. polecenie księgowania,
    b. nota księgowa,
    c. raport kasowy,
    d. dotacji,
    e. subwencji,
    f. rachunków do umów zleceń,
    g. rachunków do umów o dzieło,
    h. faktur VAT,
    i. delegacji, listę środków dla jednostek, zaliczek, rozliczeń zaliczek,
    j. listę dotacji,
    k. ryczałtów samochodowych,
    l. zaliczek stałych.
26. Moduł musi zapewniać możliwość samodzielnego definiowania kolejnych rodzajów dokumentów.
27. Moduł musi zapewniać dekretację zarejestrowanych dokumentów zarówno w zakresie zapisów księgowych jak i klasyfikacji budżetowej.
28. Moduł musi umożliwiać prowadzenie centralnego rejestru dowodów księgowych na poziomie wydziału finansowego jak również wydziałów merytorycznych.
29. Moduł powinien posiadać mechanizmy integracyjne pozwalające na pobieranie (wymianę) danych z systemów zewnętrznych takich jak:
    a. informacji o wystawionych mandatach, wraz z ich automatyczną dekretacją;

b. naliczonych list płac oraz rozliczenie podatków i składek na ubezpieczenie społeczne.
c. Import księgowań z systemów rozliczeń analitycznych takich jak: księgowość podatków, księgowość gospodarki odpadami;
d. systemu obsługi kasy;
e. ewidencji środków trwałych;
f. systemu do rozliczeń komunalnych - woda;
g. system do rozliczeń komunalnych – czynsze mieszkaniowe;
h. systemu obiegu dokumentów;
i. ewidencji koncesji alkoholowych;
j. system do planowania budżetu.

Rejestry sprzedaży i zakupów:

1. Moduł powinien zapewnić możliwość prowadzenia centralnego rejestru sprzedaży uwzględniającego możliwość wystawienia dokumentów następujących typów: faktura sprzedaży, korekta faktury sprzedaży (tryb automatyczny i ręczny), faktura do paragonu, paragon sprzedaży (obsługa drukarki fiskalnej), faktura wewnętrzna, nota obciążeniowa, rachunek.
2. Moduł powinien umożliwić prowadzenie rejestru VAT zakupów z uwzględnieniem odliczeń podatku VAT w zakresie części lub całości, zgodnie z obowiązującymi w tym zakresie przepisami z uwzględnieniem tworzenia rejestru zakupów dotyczących sprzedaży opodatkowanej oraz rejestru dotyczące sprzedaży opodatkowanej i zwolnionej.
3. Moduł powinien umożliwić wybór sposobu odliczenia podatku (wariant częściowy): przy pomocy wskaźnika, prewskaźnika lub iloczynu tych dwóch wartości.
4. Moduł powinien umożliwiać wyliczenie automatyczne korekty rocznej Vat dla zadanych wskaźników i prewskaźników rzeczywistych.
5. Moduł powinien umożliwić przyporządkowanie do dokumentu wiele zakupu klasyfikacji budżetowych celem dokonania analizy odliczeń PTU z uwzględnieniem tego kryterium.
6. Moduł powinien umożliwić dokonywania automatycznych dekretacji dokumentów handlowych (sprzedaż i zakup) za pomocą wcześniej zdefiniowanych schematów księgowań.
7. Moduł powinien umożliwić sporządzania deklaracji JPK_V7M oraz JPK_V7K (na podstawie wprowadzonych dokumentów handlowych).
8. Moduł powinien umożliwiać tworzenie zbiorów JPK w zakresach wymaganych przez ustawodawcę.
9. Moduł powinien umożliwiać agregację deklaracji cząstkowych do deklaracji łącznej w zakresie części deklaracyjnej jak i ewidencyjnej.
10. Moduł powinien umożliwić sporządzanie deklaracji VAT w zakresie obsługi wewnętrznej – deklaracja cząstkowa z zaokrągleniem do groszy oraz deklaracja zbiorcza (zagregowana) z zaokrągleniem do pełnych złotych.
11. Moduł powinien umożliwić wysyłkę deklaracji VAT i zbiorów JPK z użyciem podpisu kwalifikowanego.
12. Moduł powinien umożliwić bezpośredni zapis dokumentów wychodzących (sprzedaż) do EOD za pośrednictwem serwisu komunikacyjnego.

Rejestry umów:

Moduł musi umożliwiać katalogowanie dokumentów w przynajmniej czterech kartotekach:

a. Dokumenty dochodowe,
b. Dokumenty wydatkowe,
c. Dokumenty mieszane (dochodowo-wydatkowe),
d. Dokumenty bez kwotowe.

2. Moduł musi być powiązany integralnie z modułem **Finanse i budżet** w zakresie wspólnych słowników kontrahentów, paragrafów i zadań; kartoteka powinna umożliwić analizę stanu realizacji umowy w zakresie zaksięgowanych pozycji zaangażowania, kosztów, wydatków – powiązanie dekretacji wprowadzanych w module **Finanse i budżet** z listą umów;
3. Moduł musi posiadać wbudowane narzędzia administracyjne pozwalające na przypisywanie uprawnień użytkownikom co najmniej w zakresie dostępu do określonego wydziału, rachunku bankowego oraz rodzaju dochodu / wydatku. Możliwość przydzielania dostępu do

poszczególnych funkcji modułu np. rejestracji, akceptacji, zakańczania itp. oraz definiowania schematu numeracji umów / dokumentów.

4. Moduł musi umożliwiać rejestrację wszelkiego rodzaju umów / dokumentów, np.:
    a. umowy o dzieło,
    b. umowy zlecenie,
    c. umowy w postaci aktu notarialnego,
5. Moduł powinien współpracować z EOD w zakresie pobierania informacji o zarejestrowanych umowach: kontrahent, wartość, treść dokumentu itp.
6. Moduł musi umożliwiać rejestrację wszelkiego rodzaju umów / dokumentów, np.:
    a. umowy o dzieło,
    b. umowy zlecenie,
    c. umowy w postaci aktu notarialnego,

Obsługa wydatków:

1. Moduł musi zapewniać możliwość rejestracji różnych typów dokumentów rozchodowych i wydatkowych, w tym m.in.:
    a. rachunków do umów zleceń umożliwiając ich automatyczne składkowanie,
    b. rachunków do umów o dzieło,
    c. faktur VAT,
    d. delegacji, listę środków dla jednostek, zaliczek, rozliczeń zaliczek,
    e. listę dotacji,
    f. ryczałtów samochodowych,
    g. zaliczek stałych.
2. Moduł musi zapewniać możliwość samodzielnego definiowania kolejnych rodzajów dokumentów i rejestrów
3. Moduł musi zapewniać dekretację zarejestrowanych dokumentów zarówno w zakresie zapisów księgowych jak i klasyfikacji budżetowej.
4. Moduł musi umożliwiać prowadzenie centralnego rejestru dowodów księgowych na poziomie wydziału finansowego jak również wydziałów merytorycznych.
5. W przypadku faktur VAT, moduł musi zapewnić funkcjonalność umożliwiającą dokonanie odliczeń części lub całości podatku VAT, zgodnie z obowiązującymi w tym zakresie przepisami z uwzględnieniem tworzenia rejestru zakupów dotyczących sprzedaży opodatkowanej oraz rejestru dotyczące sprzedaży opodatkowanej i zwolnionej.
6. Moduł musi umożliwić eksport rejestrów cząstkowych z systemów innych jednostek podległych nie będących zintegrowanymi z urzędem.
7. Moduł musi umożliwić tworzenie rejestrów z uwzględnieniem korekt z różnych okresów rozliczeniowych w tym z lat ubiegłych z uwzględnieniem zachowania archiwalnych wersji poprzednich rejestrów.
8. Moduł powinien umożliwić wprowadzanie na rejestr dokumentów kosztowych w sposób ręczny i przez pobranie z EOD.
9. Moduł musi zapewniać możliwość generowania na podstawie wprowadzonych dokumentów kosztowych plików zawierających polecenia przelewów do systemu bankowego posiadanego przez Zamawiającego.
10. Procedura tworzenia paczek eksportu do systemu bankowego Zamawiającego powinna zawierać możliwość selekcji dokumentów niezapłaconych a następnie powinna posiadać (do wyboru) algorytmy grupowania np. wg daty płatności, kontrahenta itp
11. Na podstawie wprowadzonych dokumentów, moduł musi umożliwić generowanie zestawień zawierających kasową listę wypłat.
12. Moduł musi zapewnić mechanizmy, które umożliwią rejestrację dokumentu w systemie z wielostopniową akceptacją zgodnie z obowiązującymi zasadami kontroli wewnętrznej:
    a. akceptacja formalna i rachunkowa dokonywaną przez komórkę finansową,
    b. akceptacja merytoryczna, dokonywana przez komórkę merytoryczną,
    c. zatwierdzenie do realizacji przez decydentów.
13. Organizacja akceptacji musi być przejrzysta i odpowiadać drodze obiegu dokumentu.
14. Moduł musi zapewniać kontrolę dokumentu stanowiącego zobowiązanie, ze stanem realizacji umowy z kontrahentem (jeżeli umowa poprzedza dokument wydatkowy), na podstawie danych

zawartych w module rejestr umów i dokumentów, a także kontrolę tego dokumentu z planem finansowym, na każdym jego etapie, rejestracji, oraz kolejnych akceptacji w pełnej szczegółowości określonej w planie budżetu.

15. Moduł powinien umożliwić import wyciągu bankowego (ze zbioru plikowego dostarczanego przez system bankowy Zamawiającego), analizę jego danych oraz powiązanie poszczególnych wydatków z dokumentami kosztowymi na podstawie których zostały wygenerowane przelewy bankowe. Tak przygotowane dane powinny podlegać automatycznej dekretacji stosownie do podziałki budżetowej (paragrafy i zadania).
16. Moduł powinien na etapie księgowanie wyciągu bankowego analizować stan wykonania budżetu i wyświetlać stosowną informację dotycząca wychwyconego przekroczenia w zakresie planu budżetu jak i planu zawartych umów z kontrahentami.

Wymagania funkcjonalne modułu niepodatkowe wpływy budżetowe

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł musi zapewniać możliwość definiowania kontekstów pracy odpowiadającym grupom należności dla których będą tworzone kartoteki opłat (na podstawie dokumentów źródłowych), w szczególności:
    a. wieczyste użytkowanie,
    b. dochody z najmu i dzierżawy,
    c. przekształcenie prawa własności,
    d. decyzje administracyjne,
    e. inne dochody.
2. Konteksty pracy muszą mieć możliwość indywidualnej parametryzacji tzn. przypisania charakterystycznych wartości określających typ opłaty: cykliczność, czy opłata związana jest z potrzebą wystawienia faktury, domyślna stawka VAT, stawka z kartoteki towarów, sposób fakturowania (od netto/od brutto), termin płatności , schemat księgowań.
3. W skład modułu muszą wchodzić dwa elementy:
   - kontekstowa kartoteka opłat zawierająca informacje niezbędne do zidentyfikowania płatnika oraz do naliczenia wartości opłaty tworzona na podstawie dokumentów źródłowych takich jak umowa najmu, dzierżawy, decyzji itp;
   - konta księgowe będące integralną częścią systemu finansowo – księgowego (elementem zakładowego planu kont), na których będą wykonywane operacje zapisów księgowych związanych z rozliczaniem i windykacją przypisanych należności.
4. Kartoteka opłat oraz konta księgowe muszą być ze sobą powiązane w ten sposób, aby:
   - wprowadzenie nowej karty opłat musiało skutkować wygenerowaniem odpowiednika w planie kont systemu finansowo – księgowego.
   - wszystkie operacje związane z dokonywaniem zapisów księgowych muszą być wykonywane poprzez mechanizmy zaimplementowane w systemie finansowo – księgowych tzn. prowadzenie kontroli zapisów Winien - Ma z uwzględnieniem klasyfikacji budżetowej w ujęciu klasycznym (dział/rozdział/paragraf) oraz zadaniowym.
5. Moduł musi umożliwiać wprowadzanie dokumentów przez użytkowników komórek organizacyjnych z przypisaną do ich kompetencji funkcjonalnością oraz udostępnianie mechanizmów kontroli.
6. Moduł musi umożliwiać automatyczną dekretację (poprzez zdefiniowane i przypisane szablony) naliczeń zarówno w zakresie zapisów księgowych jak i klasyfikacji dochodów i wydatków budżetowych – w pełnej szczegółowości planu określonej w module planowania budżetu, będącego przedmiotem wdrożenia.
7. Moduł musi umożliwiać automatyczne wystawianie dokumentu (np. Faktury VAT) na podstawie danych z modułu rejestr umów i dokumentów.
8. Moduł musi umożliwiać wysyłanie faktur VAT w formacie PDF.
9. Moduł musi uniemożliwiać wprowadzenie modyfikacji do faktury, która została zaakceptowana i zadekretowana (system weryfikacji przez akceptację, który nie pozwoli na zmiany).
10. Moduł musi umożliwiać anulowanie faktury w przypadku, gdy nie weszła do obrotu prawnego bądź wystawić fakturę korekta jeśli jest w obrocie prawnym.

11. Dokumenty wystawione na podstawie danych z modułu rejestr umów i dokumentów muszą być kompletne i nie mogą wymuszać na operatorze ingerencji w dane. Oczywiście na żądanie operatora moduł musi umożliwiać ręczną poprawę danych w dokumencie.
12. Moduł musi uniemożliwiać wielokrotne wystawianie dokumentu na przypis wynikający z modułu rejestr umów i dokumentów (w przypadku wykorzystania całej kwoty przypisu).
13. Moduł musi umożliwiać ręczne wystawianie dokumentów oraz ich kopiowanie automatycznym wprowadzeniem do rejestru VAT.
14. Moduł musi umożliwiać wyszukiwanie kontrahenta wg wielu kryteriów (ich fragmentów), w szczególności: nazwisko, imię, adres zamieszkania, NIP, PESEL, adres (położenie) przedmiotu opodatkowania.
15. Moduł musi umożliwiać przeksięgowanie nadpłat na inną należność, możliwość zwrotu nadpłaty kontrahenta.
16. Moduł musi umożliwiać anulowanie upomnień i tytułów wykonawczych.
17. Moduł musi umożliwiać uzupełnienie oraz poprawianie daty doręczenia dla wystawionych pism (np. upomnień).
18. Moduł musi posiadać wbudowany kalkulator odsetkowy.
19. Moduł musi umożliwiać realizację kontroli naliczonych wartości opłat z zapisami księgowymi zadekretowanymi na kontach księgowych np. wyszukanie kart opłat które mają naliczoną opłatę i nie jest ona zadekretowana na koncie księgowym.
20. Moduł musi pozwalać wykonać i wydrukować rejestr wystawionych pism, np. rejestrów tytułów wykonawczych.
21. Moduł musi umożliwiać wykonywanie operacji zbiorowych na kartotekach opłat takich jak:
22. -naliczenie cyklicznej opłaty,
23. -wystawienie faktury do naliczonych opłat,
24. -zadekretować wykonane naliczenia (wygenerowanie zapisów księgowych na kontach planu kont na podstawie przypisanych szablonów dekretacji).
25. Moduł musi umożliwiać drukowanie duplikatu dokumentu do pliku PDF i wysyłanie ich za pośrednictwem modułu integrującego i systemu EOD.

Wymagania funkcjonalne modułu rozliczenia komunalne – czynsze.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł powinien umożliwiać obsługę zadań związanych z naliczaniem czynszów za lokale mieszkalne i użytkowe oraz prowadzenia szczegółowej ewidencji zawartych umów.
2. Moduł powinien umożliwiać ewidencjonowanie danych dotyczących danego lokalu ze szczególnym uwzględnieniem parametrów będących podstawą naliczenia opłaty (m.in. powierzchnia lokalu, powierzchnia użytkowa, powierzchnia grzewcza, ilość osób zamieszkujących, wyposażenie lokalu).
3. Moduł powinien umożliwiać ewidencjonowanie najemców w powiązaniu z wybranym lokalem. Kartoteka najemców powinna być wspólna z kartoteką personalną systemów dziedzinowych (moduł finansowo księgowy, system kasowy). System umożliwia wprowadzanie dat zakończenia i rozpoczęcia najmu i uwzględniać je przy naliczaniu wysokości opłaty za najem.
4. Moduł powinien umożliwiać archiwizowanie nieaktywnych kartotek.
5. Moduł powinien umożliwiać naliczanie opłaty w możliwie szerokim zakresie konfiguracji z uwzględnieniem parametrów lokalu, obowiązujących taryf oraz zużycia mediów z możliwością ich rozliczania zarówno w układzie pobierania zaliczek jak i rozliczania bezpośrednio na podstawie wskazania układu pomiarowego.
6. Moduł powinien umożliwiać wprowadzanie upustów do danej opłaty wynikające ze standardu lokalu. Wielkości upustów jak i wysokości stawek i daty ich obowiązywania wprowadzane będą przez użytkownika systemu.
7. Moduł powinien umożliwiać wprowadzanie różnych taryf(cen) dla wybranych grup budynków.
8. Moduł powinien umożliwiać wystawianie faktur z tytułu najmu pomieszczeń oraz możliwość naliczania opłaty i wydruk informacji o wysokości miesięcznej opłaty.
9. Moduł powinien umożliwiać przydzielenie do lokalu indywidualnych liczników do pomiaru mediów (gaz, prąd, woda itp.) wraz z możliwością wprowadzania ich odczytów w celu rozliczania pobranych zaliczek lub wystawiania faktur według bezpośredniego zużycia.
10. Moduł powinien umożliwiać rozliczanie ryczałtowe za media.

11. Moduł powinien umożliwiać tworzenie wydruków faktur oraz innych dokumentów w sposób masowy dla wybranych grup najemców.
12. Moduł powinien umożliwiać wydruk rejestru sprzedaży oraz zestawień opłat za zadany okres dla wybranych grup najemców.
13. Moduł powinien umożliwiać generowanie plików JPK_VAT, JPK_V7M oraz JPK_V7K.
14. Moduł powinien umożliwiać obsługę indywidualnych rachunków bankowych na które będą dokonywane płatności najemców z uwzględnieniem ich wydruku na fakturach i innych dokumentach informujących najemców o wysokości opłaty.
15. Wzory wydruków dokumentów przeznaczonych dla najemców mogą być modyfikowane w szerokim zakresie bezpośrednio z systemu. Użytkownik powinien ma możliwość dodawania do programu własnych wzorców wydruków wraz z opcją drukowania seryjnego dla wybranej grupy najemców.
16. Moduł powinien umożliwiać automatyczny zapis naliczonych zobowiązań w systemie finansowo księgowym z uwzględnieniem odpowiedniej klasyfikacji w planie kont i klasyfikacji budżetowej.
17. Z poziomu kartoteki lokalu użytkownik może mieć podgląd kartoteki rozliczeń z systemu finansowo księgowego ze szczególnym uwzględnieniem informacji o zaległościach, należnych odsetkach oraz dokonywanych wpłatach.
18. Moduł powinien umożliwiać wydruki zestawień ilościowych oraz raportów szczegółowych w zakresie naliczania opłat oraz ewidencji lokali i budynków, lokatorów.
19. Moduł powinien umożliwiać modyfikację wydruków, z uwzględnieniem parametrów w zakresie jakim naliczany jest czynsz.
20. Moduł powinien umożliwiać przygotowywanie raportu TransGUS do GUS-u.

Wymagania funkcjonalne modułu ewidencja środków trwałych.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. System musi pozwalać na szczegółową rejestrację, ewidencjonowanie posiadanego majątku w postaci: środków trwałych, wartości niematerialnych i prawnych oraz przedmiotów w użytkowaniu (małowartościowe składniki majątku).
2. System musi posiadać przejrzyste menu poprzez które można sprawnie wprowadzać nowe informacje.
3. System musi posiadać rozbudowany panel filtru pozwalający na szybkie wybranie danych z interesującego zakresu (po osobie materialnie odpowiedzialnej, miejscu użytkowania, numerze inwentarzowym).
4. System musi posiadać słownik klasyfikacji środków trwałych zgodny z obowiązującą klasyfikacją środków trwałych.
5. System musi posiadać słownik Polskiej Klasyfikacji Działalności.
6. System musi upraszczać wszelkie operacje związane z tworzeniem oraz prowadzeniem ewidencji, eliminując żmudne prace związane z ręcznym sporządzaniem kartotek, zestawień i naliczaniem amortyzacji.
7. System musi pozwalać na przyjęcie środka trwałego do ewidencji z uwzględnieniem następujących danych: numer inwentarzowy, symbol, nazwa środka. Do każdej kartoteki powinna być przypisywana faktyczna lokalizacja oraz odpowiednia klasyfikacja środka trwałego z podziałem na grupy, podgrupy i rodzaje.
8. System powinien umożliwiać przypisywanie do wprowadzonego wcześniej środka trwałego elementów zestawu. Każdy element powinien zawierać informacje takie jak: Nazwa, Miejsce użytkowania, cena.
9. System musi pozwalać na wprowadzanie danych dotyczących wartości początkowej, stopy amortyzacji, wartości umorzenia, data i numer dowodu przyjęcia, nazwisko osoby materialnie odpowiedzialnej, uwagi itp.
10. System powinien ułatwiać wprowadzanie środków trwałych oraz pozostałych środków trwałych poprzez możliwość skopiowania wprowadzonej karty środka oraz możliwość wprowadzenia zbiorczego większej ilości środków trwałych oraz pozostałych środków trwałych.
11. System musi umożliwiać dodawanie dowolnej ilości kontekstów danych w których wprowadzamy środki niezależnie od innych kontekstów. Każdy z kontekstów musi umożliwiać takie same funkcjonalności np. zamknięcie roku dla środków trwałych i pozostałych środków trwałych, naliczanie amortyzacji czy dodawanie i wydruk dokumentów.

12. System musi pozwalać na ewidencjonowanie wszystkich zdarzeń związanych ze środkami trwałymi i tworzyć dla nich odpowiednie wydruki. Musi odbywać się to w oparciu o stosowne zapisy księgowe tj.: bilans otwarcia, amortyzację miesięczną, modernizację, zmianę miejsca użytkowania, zmianę osoby materialnie odpowiedzialnej, likwidację częściową lub całkowitą, co musi pozwalać na śledzenie wszystkich operacji od zakupu środka trwałego aż do jego likwidacji.
13. System musi pozwalać na liniowy sposób amortyzacji środków trwałych.
14. System musi pozwalać na automatyczne naliczanie na cały rok kwot amortyzacji miesięcznych w układzie liniowym.
15. System musi pozwalać na aktualizację danych z automatycznym uwzględnianiem wpływu tych zmian na naliczanie amortyzacji i umorzenia.
16. System musi pozwalać na przecenę (modernizacja lub likwidacja częściowa) środka trwałego, (zmiana wartości inwentarzowej i umorzenia) z aktualizacją zmian naliczeń amortyzacji i umorzenia.
17. System musi pozwalać na likwidację środka z przeniesieniem do kartoteki środków zlikwidowanych.
18. System musi pozwalać na przywrócenie środka z kartoteki środków zlikwidowanych z automatycznym naliczeniem usuniętych amortyzacji.
19. System musi pozwalać na zakończenie roku i naliczenie bilansu otwarcia na rok następny.
20. System musi pozwalać na automatyczne naniesienie na kartoteki dokumentów amortyzacji na cały rok ewidencyjny – wykonywane podczas operacji zamknięcia roku.
21. System musi umożliwiać prowadzenie ewidencji przedmiotów w użytkowaniu w sposób ilościowy lub ilościowo – wartościowy.
22. System powinien umożliwiać uzyskiwanie na bieżąco dowolnej informacji o wybranym środku trwałym lub o grupie środków - wyświetlanie lub wydruk zestawień dla wybranych grup, działów lub obiektów np.: wykaz środków przyjętych, przekazanych pomiędzy działami lub skreślonych w danym okresie z ewidencji, zestawienie umorzeń i amortyzacji środków w danym okresie, itp. wydruki: karty środka trwałego, rejestru analitycznego, listy środków zlikwidowanych lub przyjętych do ewidencji w danym okresie sprawozdawczym, arkusz spisu z natury, oświadczenia o odpowiedzialności materialnej, wydruk zestawienia rocznego dla wszystkich grup (wartości inwentarzowe, tabele amortyzacyjne itp.).
23. System musi umożliwiać wygenerowanie sprawozdania SG01 zgodnie z wymogami GUS.
24. Po zmianie nazwy w słowniku program sam zaktualizuje ją we wszystkich składnikach majątku.
25. System musi współpracować z czytnikiem kodów kreskowych i umożliwiać elektroniczną inwentaryzację.
26. System powinien umożliwiać sporządzanie arkuszy spisów z natury.
27. System powinien umożliwiać wygenerowanie lub zapis plików w formacie PDF.
28. System powinien umożliwiać edycję wzorców wydruków.
29. System musi mieć możliwość integracji z systemem księgowości budżetowej (automatyczne tworzenie dekretów na potrzeby księgowości budżetowej).
30. System musi umożliwiać tworzenie szablonów księgowania które uwzględniają wartości brutto, umorzeń oraz netto środków trwałych.
31. System musi pozwalać na eksport danych dotyczących środków trwałych takich jak : numer inwentarzowy, nazwa, wartość, lokalizacja do pliku arkusza kalkulacyjnego lub pliku tekstowego.
32. System powinien umożliwiać przeprowadzenie automatycznej kontroli wprowadzonych danych.

Wymagania funkcjonalne modułu inwentaryzacja.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. System musi posiadać możliwość stworzenia inwentaryzacji na podstawie danych z systemu ewidencji środków trwałych według rodzaju inwentaryzowanego asortymentu (środki trwałe, pozostałe środki trwałe – wartościowe, pozostałe środki trwałe – ilościowe, wartości niematerialne i prawne).
2. System musi pozwalać na tworzenie inwentaryzacji według dwóch wybranych kluczy (miejsce, dział, obręb, osoba odpowiedzialna, komórka organizacyjna).
3. System musi umożliwiać generowanie inwentaryzacji z wyłączeniem z inwentaryzowanego asortymentu wybranej grupy środków trwałych.
4. System musi pozwalać na zatwierdzenie (zamknięcie) inwentaryzacji.
5. System musi współpracować z czytnikiem kodów kreskowych.

6. System musi współpracować z aplikacją, której funkcjonalności muszą być dostępne wyłącznie dla zalogowanych użytkowników, działającą w systemie android w wersji co najmniej 8 umożliwiając:
   a) Wysyłanie do aplikacji pliku tekstowego z danymi wygenerowanych wcześniej arkuszy inwentaryzacyjnych
   b) Wyświetlanie danych przedmiotów zawartych w arkuszach inwentaryzacyjnych
   c) Wczytanie miejsca prowadzenia inwentaryzacji
   d) Wskazanie w czasie rzeczywistym przedmiotów zinwentaryzowanych oraz nie zinwentaryzowanych poprzez pokazanie ich ilości
   e) Odebranie z aplikacji pliku w formacie .csv w celu porównania danych
   f) Wyszukiwanie arkusza inwentaryzacyjnego wg nazwy
   g) Wyszukiwanie w arkuszu przedmiotu wg nazwy
   h) Usuwanie zaznaczonych arkuszy
   i) Usuwanie zaznaczonych przedmiotów z arkusza
   j) Przekazywanie danych dotyczących przeprowadzonej inwentaryzacji za pomocą wygenerowanego pliku przenoszonego z urządzenia z aplikacją na komputer z programem Inwentaryzacja
   k) Po połączeniu z siecią – udostępnianie danych na serwerze w celu odebrania ich w programie na komputerze
7. System powinien umożliwiać po przesłaniu danych z kolektora, porównanie informacji zebranych w trakcie zaczytania czytnikiem z tymi zawartymi w bazie danych.
8. System musi umożliwiać stworzenie raportu różnic między danymi pobranymi z kolektora z danymi zawartymi w bazie danych.
9. System musi posiadać możliwość tworzenia arkuszu spisu z natury.
10. System musi umożliwiać generowanie i wydruk kodów miejsc służących do identyfikacji aktualnie inwentaryzowanego miejsca.
11. System powinien umożliwiać sporządzanie zbiorczych spisów z natury.
12. System powinien umożliwiać wygenerowanie lub zapis plików w formacie PDF.

Wymagania funkcjonalne modułu gospodarka materiałowo-magazynowa.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. System powinien umożliwiać prowadzenie ewidencji materiałów, ewidencji przychodów i rozchodów, grupowanie materiałów w magazyn, , wydruk obrotów, stanów materiałów (w tym: na początek roku, na koniec roku, na zadany dzień), obrotów dziennych i miesięcznych.
2. System powinien umożliwiać wprowadzenie nazwy dla magazynu.
3. System powinien umożliwiać integrację z modułem księgowości budżetowej w zakresie księgowania dokumentów z danego magazynu.
4. System powinien umożliwiać definiowanie słowników danych opisowych materiału i jego właściwości poprzez zdefiniowanie co najmniej: nazwy materiału, jednostkę miary, PKWIU.
5. System powinien umożliwiać wprowadzanie dokumentów aktualizujących stany magazynowe.
6. System powinien umożliwiać przeglądanie dokumentów modyfikujących stany magazynowe oraz na wprowadzanie zapisów aktualizujących przychody i rozchody.
7. System powinien umożliwiać wyszukiwanie dokumentów, co najmniej po nazwie dokumentu, nazwie materiału, dacie przyjęcia materiału, dostawcy materiału, kwocie przyjęcia.
8. System powinien umożliwiać przeglądanie ruchu na poszczególnych materiałach w wybranym magazynie.
9. System powinien umożliwiać generowanie druków i zestawień w zakresie minimum: stany; obroty; stany dzienne; stany miesięczne; stany okresowe; przychód/rozchód.
10. System musi mieć możliwość integracji z systemem księgowości budżetowej (tworzenie dekretów na potrzeby księgowości budżetowej).

Wymagania funkcjonalne modułu ewidencja mienia komunalnego.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. System powinien posiadać możliwości wyszukiwania i selekcji gruntów według dowolnego kryterium.
2. Podgląd i edycję jednostek rejestrowych, działek, budynków, lokali, innych obiektów.

3. Prowadzenie ewidencji wycen dla jednostek rejestrowych, rejestrowanie zbycia i nabycia jednostek, podziału jednostki, komunalizacji jednostki, nabycia z mocy prawa jednostki, służebności, dzierżawy, najmu, użytkowania wieczystego, zarządu, użytkowania i użyczenia.
4. Prowadzenie ewidencji wycen dla działek, postępowań, roszczeń, inwestycji i przeznaczenia.
5. Powiązanie on-line z umowami dzierżaw, najmu.
6. Funkcję zamknięcia okresu.
7. Podgląd na zapisy w programie obsługującym użytkowanie wieczyste.
8. System musi umożliwiać wystawianie faktur VAT i rachunków za czynsze dzierżawne wraz z dodatkowymi opłatami (media itp.).
9. Ewidencję dokumentów związanych z działką, zdjęć, map i innych pism w postaci elektronicznej.
10. Generowanie raportu zmian – możliwość wyszukania zmian po kolejnym imporcie danych z pliku SWDE.
11. Powiązanie systemu z ewidencją środków trwałych.
12. Generowanie zestawień: podsumowanie wg przeznaczenia, podsumowanie wg użytków, podsumowanie wg rejestrów umów dzierżaw, sprawozdanie kwartalne.
13. Generowanie informacji dotyczącej należnego od gminy podatku od nieruchomości oraz wpisywanie odpowiednich danych do formularzy podatkowych.
14. Wielopłaszczyznowa analiza wprowadzanych danych za pomocą odpowiednich zestawień.
15. System powinien umożliwiać wizualizację ewidencjonowanych działek na mapie min. w formacie , prezentowane dane powinny zawierać:
    - zbiór podstawowych danych o działce takich jak jej numer, data nabycia, sposób nabycia, numer księgi wieczystej, wartość itd.,
    - specyfikację znajdujących się na niej gruntów wraz z informacja na temat wartości poszczególnych klaso użytków,
    - informację o dzierżawach, ich typie (dzierżawa, użytkowanie wieczyste), dacie rozpoczęcia, dacie zakończenia, ewentualnych opłatach z nią związanych i harmonogramem spłat w przypadku opłat cyklicznych,
    - informacje o współwłasności i ich procentowym udziale w przypadku działek będących we współudziale,
    - informacja na temat zabudowy znajdującej się na obszarze działki, z określeniem charakteru zabudowy wraz z wartościami i opisem zabudowy wraz z rozbiciem na lokale,
    - informacja na temat sposobu zagospodarowania co daje możliwość pogrupowania działek wg w/w sposobu,
    - informację o aktualnie toczących się postępowaniach związanych z konkretnymi działkami.

Wymagania funkcjonalne modułu ewidencja koncesji alkoholowych.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Umożliwiać obsługę zadań w zakresie ewidencji i naliczania opłat za zezwolenie na sprzedaż alkoholu. Ewidencja podmiotów powinna objąć dane wnioskodawcy wraz z informacjami o lokalizacjach w których prowadzona jest sprzedaż napojów alkoholowych na terenie gminy.
2. Ewidencja musi obejmować wnioski o zezwolenia na sprzedaż napojów alkoholowych wraz z danymi wydawanych zezwoleń na sprzedaż napojów alkoholowych (sprzedaż jednorazowa/detal/gastronomia/catering) oraz na wyprzedaż napojów alkoholowych .
3. System zapewni przechowywanie informacji o wysokości sprzedaży w latach poprzednich oraz bieżącym roku wraz z informacją o ratach min. w zakresie ich wysokości i terminu płatności. Dla klientów sieciowych – podział na lokalizacje i na kategorie zezwoleń dla danej lokalizacji.
4. Ewidencja powinna umożliwiać odnotowywanie wszystkich czynności związanych z obsługą wniosku od jego przyjęcia do wydania zezwolenia oraz doręczenia decyzji.
5. W zakresie oświadczeń o wartości sprzedaży moduł musi umożliwiać ewidencjonowanie oświadczeń o wysokości osiągniętej sprzedaży z automatycznym naliczaniem opłat na następny rok.
6. Współpracę z kartoteką osób oraz kontrahentów prowadzonych w innych systemach dochodowych.
7. Zasilanie kartoteki osób z rejestru mieszkańców (ewidencji ludności).
8. Definiowanie kolejności kolumn oraz ich ukrywania na zestawieniu.

9. Tworzenie zestawień wielopoziomowych (np. I poziom zestawienie punktów – poprzez kliknięcie linku na punkcie wchodzimy do II poziomu - informacji o zezwoleniach wystawionych dla danego punktu i kolejno III poziom to raty dla danego zezwolenia).
10. Obsługę płatności masowych.
11. System umożliwi prowadzenie ewidencji wygaszonych zezwoleń.
12. System umożliwi prowadzenie ewidencji punktów którym cofnięto zezwolenia.
13. System umożliwi prowadzenie ewidencji skarg na punkt.
14. System umożliwi prowadzenie ewidencji kontroli punktów sprzedaży.
15. W zakresie obsługi wydawania zezwoleń system powinien umożliwić odnotowanie minimum w zakresie:
    - potwierdzenie przyjęcia wniosku,
    - wszczęcie postępowania,
    - skierowanie wniosku na Komisję (postanowienia, zawiadomienia, terminy),
    - wydanie decyzji zezwalającej na sprzedaż lub wydanie decyzji odmownej. , umorzenie postępowania, wygaszenie zezwolenia, a także wydanie decyzji zezwalającej na wyprzedaż, odmowy oraz tzw. decyzje zmieniające.
16. System powinien zapewnić wydruki dokumentów (decyzji) z wykorzystaniem indywidualnego edytora szablonów dokumentów.
17. System powinien posiadać mechanizm przypominający o terminach realizacji poszczególnych etapów procedury wydawania zezwolenia i naliczania opłaty.
18. System powinien zapewnić kontrolę przekroczeń i wykorzystania limitów dla poszczególnych rodzajów zezwoleń określonych w uchwale rady miasta.
19. W zakresie e-Doręczeń program powinien umożliwiać przesyłanie pism do systemu obiegu dokumentów celem ich doręczenia stronie za pośrednictwem platformy ePUAP, z wykorzystaniem mechanizmu elektronicznej skrzynki podawczej (ESP) oraz innych prawnie dopuszczalnych form doręczeń. Po stronie obiegu dokumentów tworzone będą pisma wychodzące.
20. W zakresie wniosków elektronicznych składanych za pośrednictwem platformy ePUAP oraz biznes.gov.pl, system powinien zapewnić ich automatyczne pobieranie z systemu obiegu dokumentów a następnie procedowanie elektroniczne z pobraniem metadanych zapisanych w dokumencie elektronicznym oraz jego zapis i wizualizację po jego stronie.
21. W zakresie wydawanych pism system zapewni możliwość automatycznego generowania (wydruków pism) dla przedsiębiorców uwzględniając w zakresie ich tworzenia wszystkie ewidencjonowane dane zarówno w układzie wybranego przedsiębiorcy jak i masowo dla wybranej grupy odbiorców.
22. System umożliwia generowanie wydruków na podstawie indywidualnych wzorców i ich zapis w systemie obiegu dokumentów w profilu użytkownika z uwzględnieniem typów dokumentów w nim zdefiniowanych.
23. System zapewni dodatkowo w zakresie raportowania możliwość generowania wszelkiego rodzaju zestawień/statystyk z uwzględnieniem filtrowania na podstawie wszystkich danych ewidencyjnych z uwzględnianiem stanu na określony dzień lub za wybrany okres. W szczególności system musi umożliwić raportowani w zakresie wysokości naliczonych opłat, raportu o wysokości sprzedaży alkoholu wykazanej w corocznych oświadczeniach składanych przez przedsiębiorców do 31 stycznia każdego roku.
24. System zapewni dodatkowo możliwość tworzenia własnych zestawień w oparciu o dane ewidencyjne wprowadzone do systemu.
25. System zapewni tworzenie pism do komisji rozwiązywania problemów alkoholowych.
26. System zapewni tworzenie decyzji wygaśnięcia zezwoleń.
27. System zapewni tworzenie decyzji cofnięcia zezwoleń.
28. System zapewni generowanie informacji o wysokości rat do zapłaty za korzystanie z zezwoleń w bieżącym roku.
29. System zapewni generowanie potwierdzenia dokonania opłaty za korzystanie z zezwoleń (w formie zaświadczenia)
30. System zapewni generowanie polecenia przelewu – druk dla przedsiębiorcy - sumarycznie dla wybranej raty za korzystanie z zezwoleń w danym punkcie sprzedaży.
31. System zapewni generowanie informacji o wszczęciu postępowania o cofnięcie zezwolenia.
32. System zapewni generowanie zawiadomienia o wszczęciu postępowania.

33. W zakresie raportowania powinien mieć możliwość wygenerowania raportu i wydruku przedsiębiorców którzy nie złożyli oświadczenia, z zastosowaniem filtrowania danych wg różnych kluczy obejmujących dane ewidencyjne.
34. Moduł musi umożliwiać współpracę z systemem księgowym zapewniającym prawidłowe ewidencjonowanie i egzekucję należności z tytułu wydanych pozwoleń.
35. System musi umożliwiać współpracę z systemem księgowym zapewniającym prawidłowe ewidencjonowanie i egzekucję należności z tytułu wydanych pozwoleń. System umożliwi także rozliczanie opłat – wydruk/eksport przedsiębiorców wraz z kwotą oświadczeń o wysokości sprzedaży w roku poprzednim, filtrowanie, pozycjonowanie danych.
36. W zakresie kanałów komunikacyjnych system powinien zapewnić obsługę bramki SMS z możliwością wysyłki przypomnień z pozycji kartoteki jak i korespondencji seryjnej. W tym zakresie konieczna jest możliwość podania danych dotyczących numerów telefonów komórkowych oraz możliwość odnotowania zgody na komunikację za pośrednictwem SMS-ów.
37. Zapisywanie utworzonych zestawień w formacie pdf, xls, rtf, doc.

Wymagania funkcjonalne modułu kasowego.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł musi umożliwiać kompleksową obsługę zadań w zakresie prowadzenia kasy urzędu.
2. Moduł musi w szerokim zakresie wykorzystywać możliwości środowiska Windows (przejrzyste wydruki graficzne, czytelnia forma prezentacji, rozbudowane metody selekcji danych, przyjazny interfejs itp.).
3. Moduł musi umożliwiać przyjmowanie wpłat i wypłat na wybrane raporty kasowe, wydawanie dokumentów KP, KW, PO, BD itp.
4. Moduł musi umożliwiać dwukierunkową współpracę z pozostałymi systemami rozliczającymi dochody budżetowe.
5. Moduł musi umożliwiać generowanie raportów kasowych oraz okresowych zestawień z możliwością ich dowolnego filtrowania.
6. Moduł musi posiadać obsługę kodów kreskowych umieszczanych na wydrukach z systemów rozliczających dochody budżetowe (np. nakazy płatnicze w systemie podatkowym).
7. Moduł musi pozwalać na identyfikację płatnika za pomocą czytnika kodów kreskowych.
8. Moduł musi pozwalać na współpracę zarówno z tradycyjnymi drukarkami igłowymi jak i drukarkami atramentowymi czy laserowymi.
9. Moduł musi dawać możliwość samodzielnego tworzenia i modyfikowania wzorów wydruków za pomocą wbudowanego edytora tekstu.
10. Moduł musi pozwalać na integrację z wszystkimi modułami księgowymi umożliwiając automatyczną obsługę kasową płatności zobowiązań.
11. System musi zapewnić obsługę e-usług w zakresie niezbędnym do ich realizacji.

Wymagania funkcjonalne modułu kadrowo-płacowego.

KADRY – moduł musi spełniać następujące wymagania funkcjonalne:

Wymagania ogólne.

1. Moduł musi obsługiwać zatrudnionych pracowników oraz podległych kierowników jednostek organizacyjnych, zleceniobiorców, stypendystów, radnych, członków komisji działających w jednostce
2. Moduł nie może blokować pracy w module kadrowym w czasie naliczania listy płac.
3. Moduł musi umożliwić przeprowadzenie zmian w strukturze organizacyjnej:
   a) zmiana dostępnych danych jednostki
   b) zmiana nazwy jednostki,
   c) utworzenie nowej komórki organizacyjnej, system musi zapewnić możliwość definiowania nowych komórek organizacyjnych w strukturze organizacyjnej z datą obowiązywania i kodem zgodnym z regulaminem organizacyjnym jednostki. Struktura organizacyjna może się zmieniać, dlatego musi być możliwość określenia czasu (data od, do) jego obowiązywania,
4. W Module domyślnie musi być widoczna aktualna struktura organizacyjna.
5. Moduł musi w formie graficznej przedstawiać strukturę jednostki w formie drzewa.
6. Użytkownik, poprzez wybór odpowiedniej opcji, zgodnie z przyznanymi uprawnieniami, musi mieć dostęp do wybranych struktur,
7. Przy raportach muszą być uwzględniane dane z aktualnych i archiwalnych komórek.

8. Moduł musi umożliwiać odnotowanie adresu płatnika, informacji o nr NIPie, nr REGON, kontach bankowych.
9. Moduł musi posiadać możliwość definiowania formatu numerowania pism z wykorzystaniem jednolitego rzeczowego wykazu akt???. Można by to rozbudować
10. Moduł musi umożliwiać ustawianie domyślnego kalendarza.
11. Moduł musi umożliwiać odnotowanie danych osoby reprezentującej jednostkę.
12. Moduł musi domyślnie wyświetlać dane aktualne, zawarte w bieżącym czasookresie.
13. Moduł musi umożliwiać ewidencjonowanie danych osobowych pracownika.
14. Moduł musi sprawdzać poprawność naniesionego Nr PESEL.
15. Moduł musi sprawdzać czy nanoszony nr PESEL już występuje w bazie danych. Jeśli nastąpi powtórzenie nr PESEL system powinien o tym poinformować.

Przypominacz.

16. Moduł podczas uruchomienia aplikacji będzie informować użytkownika o zbliżających się terminach, np.
    a) Wygasających umowach o pracę,
    b) końca ważności podstawowych badań lekarskich,
    c) końca ważności dodatkowych badań lekarskich,
    d) końca ważności szkoleń BHP,
    e) upłynięcia terminu orzeczenia o niepełnosprawności,
    f) nabycia prawa do dodatku za wysługę lat,
    g) zmiany wymiaru urlopu wypoczynkowego,
    h) nabycia uprawnienia do nagrody jubileuszowej,
    i) nabyciu przez pracownika uprawnień emerytalnych,
    j) kończących się urlopach bezpłatnych, wychowawczych,
    k) pracownikach, którzy przebywają na ciągłej absencji chorobowej dłuższej niż 30 dni - kontrolne badania lekarskie,
    l) daty ważności notatki,
    m) daty zmiany szablonu kalendarza.

    Moduł podczas uruchomienia aplikacji będzie informować użytkownika o zbliżających się terminach, np.
17. „Przypominacz" musi swoim działaniem objąć czasokres bieżącego miesiąca w raz z następnym miesiącem.

Wyszukiwanie pracowników

18. Moduł musi umożliwić wyszukiwanie pracowników w szczególności po:
    a) nazwisko, imię, PESEL, NIP, Nr ewidencyjnym, Nr akt
    b) strukturze organizacyjnej w której jest zatrudniony,
    c) stanowisku,
19. Moduł musi umożliwić filtrowanie danych zawartych w kadrach na podstawie jednego, kilku bądź kilkunastu wybranych parametrów System musi umożliwić wydrukowanie takich informacji.

Raportowanie

20. Moduł musi umożliwiać wydruk wszystkich zawartych w nim danych oraz umożliwić segregowania na różnych poziomach: jednostka, komórka organizacyjna (departament, wydział/biuro/ samodzielna komórka organizacyjna na prawach wydziału, oddział/zespół), stanowisko, ds. ... itp., sortowanych wg różnych pól w zależności od potrzeb użytkownika

Dane pracownika

21. Moduł musi zapewniać przechowywanie historycznych danych osobowych m.in. okresów ważności badań lekarskich, dokumentów tożsamości oraz historycznych danych o warunkach zatrudnienia pracownika m.in. zajmowanego stanowiska, komórki organizacyjnej, przyznanych składnikach wynagrodzeń oraz ich wysokości, wymiaru etatu itd.
22. Podczas wprowadzania nowego pracownika do Moduł, Moduł musi sprawdzić czy w bazie danych nie istnieje już osoba o tym samym numerze PESEL, W takim przypadku Moduł musi rozszerzyć kartotekę takiego pracownika o kolejne zatrudnienie. Moduł nie powinien zakładać nowej kartoteki.

23. W przypadku pracownika znajdującego się w Systemie w związku z wcześniejszym zatrudnieniem w danej jednostce w ramach umowy o pracę (powołania) wyboru System musi: edytować wcześniej wpisane dane, umożliwić ich aktualizację oraz podpięcie danemu pracownikowi kolejnego zatrudnienia w ramach umowy o pracę (powołania) wyboru.
24. Przy wprowadzaniu danych Moduł musi umożliwić oznaczenie/wpisanie poniżej wskazanych danych:
    a) czy jest to pierwsze zatrudnienie w życiu (tak/nie),
    b) czy jest to zatrudnienie w wyniku naboru,
    c) czy jest to zatrudnienie po raz pierwszy na stanowisku urzędniczym ,
    d) liczby dni absencjach wykorzystanych u poprzedniego pracodawcy w roku, w którym następuje zatrudnienie, m. in.: urlopu wypoczynkowego (w tym urlopu na żądanie), dodatkowego urlopu, dni/ godzin wolnych przysługujących na podst. art. 188 kp., dni za które wypłacono wynagrodzenie za czas choroby (art. 92 kp.).
25. Wprowadzone dane muszą być automatycznie przetworzone i uwzględnione przez moduł Kadrowy w następujących zakresach działania:
    a) przy naliczaniu przysługujących urlopów, w tym uprawnień do urlopu w pierwszym roku pracy, dni z tytułu opieki nad dzieckiem,
    b) w sprawozdaniach GUS,
    c) przy ustalaniu prawa do dodatkowego wynagrodzenia rocznego ("13").
26. Moduł musi pozwolić na wprowadzenie i edytowanie wszystkich danych osobowych, w szczególności:
    - Nazwisko,
    - Imię,
    - Drugie imię,
    - Nr Pesel, Daty Urodzenia,
    - Miejsca Urodzenia,
    - Płci,
    - Nr NIP,
    - Nr dowodu osobistego, przez kogo został wydany, data wydania,
    - Urząd skarbowy,
    - Kod oddziału NFZ,
    - Informację o zgodzie lub sprzeciwie o przetwarzaniu danych w celach marketingowych oraz ich przekazywania innym administratorom d
27. Moduł musi pozwolić na wprowadzenie i zmianę danych dotyczących służby wojskowej.
28. Moduł musi pozwolić na wprowadzenie i edytowanie danych adresowych: zameldowania, zamieszkania, korespondencyjny, kontaktowych: telefon, email.
29. Moduł musi zapewnić możliwość wprowadzenia oraz edycję danych osoby, którą należy powiadomić w razie wypadku.
30. Moduł musi pozwolić na wprowadzenie i edytowanie danych dotyczących wykształcenia: poziom wykształcenia, uzyskany tytuł, ukończona szkoła (nazwa, rok ukończenia, uzyskane wykształcenie - kierunek, specjalność.
31. Moduł musi pozwolić na wprowadzenie i edytowanie danych: znajomość języków obcych (nazwa, oraz stopień znajomości języka w oparciu o następujące kryteria – w mowie, w piśmie, czytanie),
32. Moduł musi pozwolić na wprowadzenie i edytowanie ukończonych kursów/szkoleń/studia podyplomowe (data, rodzaj),
33. Moduł musi umożliwić rejestrowanie orzeczenia o niepełnosprawności danego pracownika: stopień niepełnosprawności (lekki, umiarkowany, znaczny), kod rodzaju niepełnosprawności (np. 03-L, 05-R, 10- N, 11-I itd.), oznaczenie orzeczenia o schorzeniu szczególnym, które obniża wskaźnik zatrudnienia osób niepełnosprawnych, okres, na który został orzeczony, data doręczenia orzeczenia pracodawcy).
34. Wprowadzona informacja o umiarkowanym i znacznym stopniu niepełnosprawności musi mieć odzwierciedlenie w normie czasu pracy, w urlopach, czyli ustalenie prawa do dodatkowego urlopu oraz naliczenie jego wymiaru., przez co należy rozumieć dostosowanie przez System wymiaru czasu pracy, urlopów i innych, wynikających z przepisów prawa, parametrów.
35. Moduł musi umożliwić zarejestrowanie informacji o przynależności do NFZ (kod, pełna nazwa).
36. Moduł musi umożliwić zarejestrowanie świadczenia ZUS (uzyskane prawa do emerytury lub renty, data od - do, jednostka ZUS).

37. Moduł musi pozwolić na wprowadzenie i edytowanie danych o członkach rodziny: imiona, nazwisko, data urodzenia, PESEL, datę urodzenia stopień pokrewieństwa, uczy się (tak, nie, nie dotyczy), wspólne gospodarstwo (tak, nie, nie dotyczy), stopień niepełnosprawności, uprawnienia zdrowotne: (tak, nie, nie dotyczy), data uzyskania, data utraty, adres zamieszkania (jeżeli jest zgodny z adresem pracownika to system powinien pobierać informacje z danych pracownika, w przeciwnym wypadku musi istnieć możliwość ręcznego wprowadzenia adresu.
38. Raz wprowadzone dane do Modułu o członkach rodziny muszą być widoczne w każdym kolejnym zatrudnieniu w danej jednostce z ewentualną możliwością ręcznej korekty.
39. Moduł musi dać możliwość wprowadzenia numeru ewidencyjnego pracownika.
40. Moduł musi umożliwić rejestrowanie całego przebiegu pracy zawodowej pracownika takie jak, poprzednie zatrudnienia (zaliczane odrębnie do: stażu pracy tj. do dodatku za wieloletnią pracę, nagrody jubileuszowej, do wymiaru urlopu, prawa do urlopu, do emerytury/renty, do stażu zakładowego) - daty od - do, wskazanie ilości lat miesięcy i dni trwania danego zatrudnienia - (wyliczenie dni kalendarzowych), nazwa instytucji, okresy wyłączone (urlopy bezpłatne itp.), praca na gospodarstwie rolnym, odbyte staże, czasokresy zasiłków wypłacanych przez Urzędy Pracy, służba wojskowa.
41. Moduł musi przeliczać staż ze wskazaniem sumy przepracowanych: lat, miesięcy i dni zaliczanych/wyłączonych do ww. uprawnień. Wskazanie ww. sumy na dzień zatrudnienia oraz aktualnie na dzień podglądu.
42. Moduł musi przeliczać staż zakładowy pracownika (suma aktualnego oraz suma okresu wyłączonego ze stażu zakładowego - okres trwania urlopu bezpłatnego itp.).
43. Moduł musi dostarczyć funkcjonalność pozwalającą na obliczenie wysokości dodatku za wieloletnią pracę wskazujący wysokość dodatku na podaną datę oraz wyliczenie daty, od której liczony jest staż pracy.
44. Moduł musi zawierać panel informacyjny, na którym będzie widoczna informacja na temat poprzedniego zatrudnienia raz z bieżącym zatrudnieniem w postaci:
    - Okresu zatrudnienia,
    - Nazwy zakładu pracy,
    - Informacji o czasie zatrudnienia w notacji: lata miesiące, dni z wyszczególnieniem okresów: Prawa do urlopu, Ogólna wysługa lat, Prawo do emerytury, Wysługa zakładowa, Jubileusz wysługa.
45. Moduł musi umożliwić wygenerowanie i wydruku kart stażu zaliczanego do:
    a) dodatku za wieloletnią pracę,
    b) nagrody jubileuszowej,
    c) urlopu wypoczynkowego,
    d) emerytury/renty,
    e) zakładowego stażu pracy.
46. Moduł musi zapewnić możliwość wprowadzenia oraz edycję danych dotyczących ukończonych szkół, a w szczególności takich jak:
    - Nazwa szkoły,
    - Typ szkoły,
    - Zawód wyuczony,
    - Okres pobierania nauki,
    - Ilość lat zaliczanych do wyliczenia prawa do urlopu wypoczynkowego.
47. Moduł musi rejestrować dane dotyczące ważności podstawowych badań lekarskich - rodzaj badań: wstępne/ okresowe/ kontrolne/, od kiedy, do kiedy. W przypadku upływu terminu badań okresowych System musi sygnalizować brak ważnych badań lekarskich.
48. Moduł musi rejestrować dane dotyczące ważności dodatkowych badań lekarskich - specjalistyczne, od kiedy, do kiedy. W przypadku upływu terminu badań dodatkowych System musi sygnalizować brak ważnych badań lekarskich.
49. Kod tytułu ubezpieczenia, musi być tworzony automatycznie przez System w wyniku przetworzenia wcześniej wpisanych przez użytkownika danych.
50. Moduł musi generować do programu PŁATNIK zgłoszenie/wyrejestrowanie pracownika/ zleceniobiorcy do ubezpieczenia społecznego i zdrowotnego oraz członków rodziny do ubezpieczenia zdrowotnego - wprowadzone w Systemie dane winny być automatycznie pobierane do zgłoszenia/wyrejestrowania. System musi pozwalać na wygenerowanie do programu PŁATNIK

zmiany/korekty w danych osobowych pracownika/ zleceniobiorcy oraz wyrejestrowania i nowe kolejne zgłoszenia członków rodziny w związku z wprowadzeniem zmian w danych wpisanych do Systemu, które Płatnik zobowiązany jest zgłosić do ZUS.

51. Moduł musi umożliwić określenie statusu umowy/aneksu - propozycja/zatwierdzony.
52. W przypadku określenie statusu umowy/aneksu - propozycja - naniesione zmiany mogą być widoczne wyłącznie w Module Kadry.
53. Moduł musi umożliwić przypisanie pracownika do komórki organizacyjnej, w której jest zatrudniany (wybieranej z wprowadzonego do Systemu drzewa organizacyjnego): nazwa komórki organizacyjnej.
54. Moduł musi umożliwić wprowadzenie rodzaju umowy:
    a) na czas nieokreślony,
    b) na czas określony,
    c) umowa do dnia porodu z datą od - bez wskazania daty zakończenia umowy,
    d) umowa na czas określony w celu zastępstwa innego pracownika, wskazanie danych pracownika zastępowanego, daty od, bez wskazania daty zakończenia umowy,
    e) umowa na czas trwania projektu z datą od, do,
55. Moduł musi umożliwiać ewidencjonowanie umów o pracę, aneksów, angaży, a w szczególności musi umożliwiać gromadzenie danych takich jak:
    - Rodzaj umowy,
    - Data umowy,
    - Sposób rozwiązania umowy,
    - Przypisanie do komórki organizacyjnej,
    - Zajmowane stanowisko służbowe,
    - Pełniona funkcja służbowa,
    - Przynależność do grupy zatrudnionych,
    - Wymiar etatu,
    - Typ obowiązującej pracownika stawki (wynagrodzenie miesięczne, wynagrodzenie godzinowe),
    - Składniki wynagrodzenia z możliwością określenia wartości, daty obowiązywania składnika, kategorii zaszeregowania,
    - Wartość procentowa i kwotowa wysługi lat (dodatek stażowy) musi być wyliczana automatycznie.
56. W warunkach zatrudnienia musi być możliwość wprowadzenia określenia rodzaju zatrudnienia (umowa o pracę, powołanie, wybór).
57. Moduł musi umożliwić przypisanie pracownikowi właściwego kalendarza pracy.
58. Moduł musi umożliwić wprowadzenie następujących danych związanych ze składnikami wynagrodzenia:
    a) wynagrodzenie zasadnicze - kategoria zaszeregowania, kwota w zł,
    b) dodatek funkcyjny – stawka lub kwota w zł,
    c) dodatek służbowy,
    d) dodatek specjalny (data od - data do, kwota w zł.),
    e) nagrody,
    f) inne określone w regulaminie wynagrodzenia
59. Moduł musi umożliwić rejestrowanie kar i wyróżnień z informacjami:
    a) kary: rodzaj kary (nagana, upomnienie, kara pieniężna), data udzielenia, kto przyznał, kwota,
    b) wyróżnienie: rodzaj wyróżnienia (nagroda pieniężna, pochwała, dyplom), data przyznania, kto przyznał, kwota, data wypłaty.
60. Moduł musi pokazywać daty nabycia uprawnień do nagrody jubileuszowej. Informacja musi zawierać: jednoznaczne określenie stopnia nagrody, daty nabycia nagrody.
61. Moduł musi rejestrować następujące informacje o zwolnieniach lekarskich: rodzaje absencji, seria oraz numer zwolnienia, data od - do, pozostałe dane jak dni absencji powinny być wyliczane automatycznie, dodatkowo moduł powinien mieć możliwość określenia szczegółów zwolnienia chorobowego taki jak: wynagrodzenie chorobowe, zasiłek chorobowy, Zasiłek chorobowy – wypadek w pracy lub w drodze do pracy, chorobowe w ciąży.
62. Moduł musi mieć możliwość automatycznego importowania danych z e-zwolnień lekarskich udostępnionych na profilu informacyjnym Pracodawcy (Płatnika) znajdującego się na Platformie Usług Elektronicznych ZUS (PUE ZUS) do ewidencji absencji pracownika.
63. Moduł musi rejestrować wszystkie rodzaje absencji, które mogą wystąpić w jednostce, z uwzględnieniem: rodzaju absencji, daty od – do, oraz absencji godzinowej.

64. Moduł musi kontrolować wymiary absencji: urlopy, zwolnienie od pracy udzielane na podst. art. 188 kp., wyszczególnienie urlopów na żądanie (limit 4 dni w roku kalendarzowym zdejmowanych z urlopu bieżącego).
65. Moduł musi umożliwić wpisanie dwóch absencji w jednym okresie np. w zbiegu wyjścia prywatnego w godzinach porannych i opieki nad zdrowym dzieckiem w godzinach popołudniowych.
66. Moduł musi umożliwić korygowanie błędnie wprowadzonych nieobecności.
67. W przypadku absencji, których czas trwania narzucany jest przez przepisy prawa, System samodzielnie musi wstawiać maksymalną datę końcową (np. urlop macierzyński, urlop ojcowski) z możliwością wprowadzenia ręcznej korekty.
68. Po wpisaniu absencji, które zgodnie z prawem powodują zawieszenie stosunku pracy (np.: urlop bezpłatny) System musi odliczać je automatycznie ze stażu pracy.
69. W Module muszą być rejestrowane informacje dotyczące wypracowanych nadgodzin w postaci: rodzaj nadgodzin, ilość, data wypracowania, rozróżnienie sposobu rozliczenia (do odbioru, do wypłaty).
70. W Module muszą być rejestrowane absencje godzinowe np. odbiór nadgodzin, urlop godzinowy (w przypadku pracowników niepełno etatowych), wyjść prywatnych. Informacja musi zawierać datę absencji, rodzaj, ilość godzin, data wypracowania odbieranych nadgodzin w przypadku odbioru nadgodzin.
71. Moduł powinien automatycznie prowadzić bilans godzin do odebrania w przypadku godzin nadliczbowych, które nie są wypłacane oraz godzin do odpracowania w przypadku wystąpienia wyjść prywatnych.
72. W Module musi być możliwy szybki podgląd sumy liczby absencji (z podziałem na rodzaje) oraz w wybranym czasokresie.
73. Moduł musi umożliwić rejestrowanie pracę w dniu wolnym z tytułu pięciodniowego tygodnia pracy/ w niedzielę/ w święta.
74. Moduł musi zapewnić możliwość prowadzenia dowolnych kalendarzy w zakresie danych:
    - Nazwa (opis) kalendarza,
    - Definicji dowolnych dni roboczych,
    - Definicji w sposób dowolny godzin roboczych.
75. Tworzenie nowego miesiąca dla kalendarza musi odbywać się na podstawie uprzednio zdefiniowanych domyślnych godzin pracy urzędu lub na podstawie szablonu kalendarza.
76. Na podstawie kalendarzy oraz słownika kodów nieobecności musi być tworzony szczegółowy wykaz czasu pracy dla pracownika.
77. Kalendarze muszą mieć postać graficzną, z wyszczególnieniem absencji w postaci określonego koloru.
78. Moduł musi zawierać automat przypisujący cechy kalendarza pracownikom lub grupom pracowników.
79. Moduł musi posiadać skróty klawiszowe służące do szybkiego nanoszenia nieobecności.
80. Moduł musi posiadać możliwość naniesienia całego okresu absencji podczas jednego działania użytkownika.
81. Moduł musi umożliwiać edycję oraz usuniecie naniesionych informacji dotyczących absencji pracownika.
82. Moduł musi umożliwiać naniesienie wyjść prywatnych pracownika w notacji godzinowej oraz minutowej.
83. Moduł musi umożliwiać ewidencję następujących urlopów:
    - Urlopu wypoczynkowego,
    - Urlopu na żądanie,
    - Urlopu szkolnego,
    - Dni opieki nad zdrowym dzieckiem,
    - Urlopu wychowawczego.
84. Moduł musi umożliwiać ewidencjonowanie bieżącego i zaległego urlopu wypoczynkowego.
85. Moduł musi umożliwiać definicję innego typu urlopu.
86. Moduł musi umożliwiać prowadzenie planu urlopowego.
87. Musi być możliwość drukowania pustych i wypełnionych formularzy z planowanym urlopem wypoczynkowym. Dodatkowo musi być możliwość śledzenia:
    - Urlopu wypoczynkowego,

- Urlopu na żądanie,
- Urlopu szkolnego,
- Dni opieki nad zdrowym dzieckiem,
- Urlopu wychowawczego.

88. Moduł musi automatycznie ustalić prawo do urlopów - wskazać datę oraz wyliczać wymiar urlopów z ewentualną możliwością ręcznej modyfikacji.
89. W przypadku zmiany wymiaru urlopu wypoczynkowego w trakcie zatrudnienia, System musi automatycznie wyliczyć wymiar i wskazać datę zmiany z ewentualną możliwością ręcznej modyfikacji.
90. Moduł musi przeliczać automatycznie, z możliwością ręcznej modyfikacji, liczbę przysługującego pracownikowi dni urlopu w związku z zakończeniem okresu zawieszenia stosunku pracy (urlopu bezpłatnego, urlopu wychowawczego).
91. Dla osób zatrudnionych na czas określony System musi naliczać liczbę dni urlopu przysługującego pracownikowi proporcjonalnie do czasu trwania umowy.
92. Dla wszystkich rodzajów urlopów (wypoczynkowego, dodatkowego przysługującego z tytułu niepełnosprawności, uprawnień kombatanckich, podnoszenia kwalifikacji zawodowych np. studia doktoranckie, aplikacja radcowska) System musi pokazywać informacje:
    a) wymiar urlopu przysługujący w danym roku,
    b) ilość urlopu aktualnego: dni/godziny,
    c) ilość urlopu zaległego dni/godziny,
    d) ilość urlopu do wykorzystania dni/godziny,
    e) ilość dni urlopu na żądanie (do wykorzystania oraz wykorzystanych),
    f) liczbę dni zwolnienia od pracy z tytułu opieki nad dzieckiem do lat 14 (do wykorzystania/ wykorzystanych),
    g) liczbę dni przysługującego ekwiwalentu (dla zakończonych stosunków pracy).
93. Moduł musi pozwolić na ręczną modyfikację przez uprawnionego użytkownika powyższych informacji.
94. Raport o stanie urlopów musi być wykonywany na wybrany przez użytkownika dzień.
95. Moduł musi umożliwić zapisywanie informacji: data rozwiązania stosunku pracy, tryb rozwiązania stosunku pracy (wybierany ze słownika), kod ZUS dotyczący przyczyny zakończenia okresu ubezpieczenia społecznego.
96. Moduł musi automatycznie wyliczać liczbę dni/ godzin urlopu, za który przysługuje ekwiwalent.
97. Moduł musi umożliwiać rejestrację ryczałtów samochodowych, w zakresie danych:
    - Data przyznania ryczałtu,
    - Okresu, na który został przyznany ryczałt samochodowy,
    - Numer silnika,
    - Marki samochodu,
    - Numeru rejestracyjnego,
    - Pojemności silnika,
    - Rok produkcji samochodu,
    - Informację o przyznanym limicie kilometrów,
    - Kwota ryczałtu.
98. Moduł musi umożliwiać na podstawie danych o ryczałcie samochodowym wygenerowanie rachunku ryczałtu samochodowego
99. Moduł musi posiadać aktówkę pracownika w której umieszczane muszą być wszystkie dokumenty elektroniczne dotyczące pracownika. Dokumenty te muszą być generowane w oparciu o szablony dokumentów. Musi być możliwość pobrania obrazu bezpośrednio ze skanera, np. badania lekarskie, które dostarczył pracownik lub dołączyć dokument znajdujący się na dysku komputera.
100. Moduł musi zawierać możliwość prowadzenia ewidencji okresowego rozliczania wydawanych pracownikom środków ochrony indywidualnej (odzież ochronna i robocza) wraz z możliwością wykonania imiennego zestawienia wydanych środków ochrony indywidulanej.
101. Moduł musi zawierać możliwość stworzenia zestawienia zapotrzebowania środków ochrony indywidualnej.

Raportowanie

102. Moduł musi generować świadectwo pracy z możliwością modyfikowania (zgodnie z przepisami

prawa) automatycznie pobierając niezbędne informacje z części kadrowej i płacowej m. in. liczba dni, za które pracownik otrzymał wynagrodzenie zgodnie z art. 92 kp. w roku kalendarzowym, w którym ustał stosunek pracy, zajęcia sądowe (oznaczenie komornika i numer sprawy egzekucyjnej oraz wysokość potrąconych kwot).

103. Moduł musi udostępniać edytowalne pole notatek, przypisane do kartoteki danego pracownika, gdzie Zamawiający będzie miał możliwość wpisywania informacji dodatkowych m.in.: zakresy czynności, zmiany godzin pracy. Notatka musi być ograniczona datami obowiązywania i połączona z systemem Alertów
104. Moduł musi umożliwić generowanie kompletnej umowy o pracę automatycznie wybieranej przez System w zależności od rodzaju umowy. Przy generowaniu umowy o pracę System musi automatycznie pobierać i przetwarzać wszystkie niezbędne dane wprowadzone do Systemu.
105. Moduł o pracę musi być automatycznie wypełniana przez Moduł odpowiednimi do danego rodzaju umowy danymi znajdującymi się w Systemie.
106. Moduł musi generować „Informację do umowy o pracę", w której znajdują się m. in. informacje określone w art. 29 § 3 kp. Przy generowaniu „Informacji do umowy o pracę" System musi automatycznie pobierać, przetwarzać wszystkie niezbędne dane wpisane do Systemu i umieszczać w jej treści informacje np.:
    a) obowiązującej pracownika dobowej i tygodniowej normie czasu pracy (w przypadku pracowników zatrudnionych w niepełnym wymiarze czasu pracy System musi wskazywać również rozkład czasu pracy tj. dni robocze oraz dzienną ilość godziny pracy w tygodniu - dane pobierane z przypisanego pracownikowi kalendarza),
    b) o wymiarze urlopu oraz proporcjonalnej ilości dni urlopu (wypoczynkowego, dodatkowego) przysługującego pracownikowi,
107. Moduł musi umożliwić wprowadzenie informacji o zakresie obowiązków poszczególnych pracowników. Informacje muszą być wprowadzane z wykorzystaniem słownika definiowanego samodzielnie przez Zamawiającego.
108. Użytkownik musi mieć możliwość generowania wydruków dla wybranego pracownika z wszystkich informacji znajdujących się w Systemie, w szczególności:
    a) Wykazu wypłaconych pracownikowi nagród w okresie od - do.
    b) Wykazu dokonanych zmian wynagrodzenia w okresie od - do.
    c) Wykazu absencji w okresie od-do (z możliwością obcięcia absencji na podane daty od-do), rodzaje absencji do wyboru itp.
    d) Karty stażu pracy m.in.: ogólnego stażu pracy, stażu przed zatrudnieniem, stażu do nagrody jubileuszowej, stażu do emerytury/renty, stażu zakładowego, stażu do urlopu.
    e) Karty ewidencji czasu pracy w okresie od -do.
    f) Zaświadczenia o zatrudnieniu: dane pracownika z danymi o samym zatrudnieniu (m.in.: imię i nazwisko, adres zamieszkania/ zameldowania, data zatrudnienia, jednostka, stanowisko, etat, rodzaj umowy: czas określony/nieokreślony, ze wskazaniem czasu trwania umowy w przypadku umów na czas określony oraz danych pracownika zastępowanego w przypadku umów na zastępstwo) z możliwością wprowadzanie ręcznych modyfikacji i pobrania innych danych znajdujących się w Systemie.
    g) Zaświadczenia o wykorzystywanym przez pracownika urlopie wychowawczym, bezpłatnym z możliwością wprowadzanie ręcznych modyfikacji i pobrania innych danych znajdujących się w Systemie.
    h) Zaświadczenia dla ZUS z danymi o okresach nieskładkowych, urlopach bezpłatnych, wychowawczych.
    i) Przebiegu zatrudnienia pracownika w jednostce (historia) z wyszczególnieniem m.in. zajmowanych stanowisk, komórek organizacyjnych, w których był i jest zatrudniony pracownik.
109. Moduł musi umożliwić wykonanie raportów ze wszystkich informacji znajdujących się w Systemie dotyczących wszystkich pracowników jednostki, danej komórki. Użytkownik musi mieć możliwość konfigurowania wydruków: alfabetycznie nazwiskami/stanowiskami z podsumowaniem wybranych danych w określonej jednostce, jak również wydruki samych podsumowań. Dodatkowo użytkownik musi mieć możliwość budowania szczegółowych zapytań i warunków przy definiowaniu raportów.
110. Moduł musi umożliwić generowanie raportów w różnych konfiguracjach z wszystkich elementów znajdujących się w Systemie wg stanu na określony dzień lub w przedziale czasowym (z możliwością wyboru: pracowników zwolnionych, pracowników aktualnie zatrudnionych), w szczególności:

a) zatrudnieni Pracownicy z możliwością podziału na czas określony i nieokreślony,
b) wynagrodzenia pracowników,
c) zmiany wynagrodzeń w okresie,
d) pracownicy np.: wg wykształcenia, wieku, płci, miejsca zamieszkania, stażu pracy, posiadanych dzieci, daty zatrudnienia, ukończonych kursów i szkoleń, znajomości języków,
e) struktura wieku, wykształcenia na dzień,
f) zwolnieni Pracownicy w okresie od - do,
g) pracowników, którzy zostali zatrudnieni w okresie od - do,
h) pracownicy z orzeczoną niepełnosprawnością, z możliwością wyboru stopnia niepełnosprawności: znaczny / umiarkowany / lekki,
i) przebieg zatrudnienia pracowników w jednostce (historia) z wyszczególnieniem m.in. zajmowanych stanowisk, komórek organizacyjnych zatrudniających pracownika,
j) pracownicy z ustalonym prawem do emerytury/renty,
k) pracownicy, którzy nabędą uprawnienia do emerytury w określonym czasie,
l) pracownicy, którzy nabędą uprawnienia do emerytury w określonym czasie z wskazaniem wynagrodzeń miesięcznych oraz z wyliczeniem kwoty przysługującej odprawy,
m) pracownicy, którym przyznano nagrody, udzielono kar,
n) ważność badań lekarskich,
o) uprawnieni do nagrody jubileuszowej, dodatku za wieloletnią pracę we wskazanym okresie,
p) uprawnieni do nagrody jubileuszowej, dodatku za wieloletnią pracę we wskazanym okresie z podaniem wynagrodzeń miesięcznych oraz z wyliczeniem kwoty przysługującego świadczenia,
q) lista pracowników uprawnionych i nieuprawnionych do dodatkowego wynagrodzenia rocznego z możliwością modyfikacji,
r) przegląd absencji,
s) wypracowanych nadgodzin,
t) pracy w dniu wolnym,
u) pracy w niedzielę I święta,
v) wyjść prywatnych,
w) odpracowań wyjść prywatnych,
x) czas pracy w danej komórce organizacyjnej,
y) rozliczone nadgodziny - odebrane/zapłacone,
z) nierozliczone nadgodziny,
aa) nieoddanych dni wolnych,
bb) karta ewidencji czasu pracy,
cc) alfabetyczna lista obecności pracowników komórek organizacyjnych/wewnętrznych komórek organizacyjnych,
dd) ilość dni wynagrodzenia chorobowego,
ee) ilość dni zasiłku chorobowego,
ff) wprowadzone zwolnienia lekarskie,
gg) zwolnień dłuższych niż.,
hh) urlopy wypoczynkowe w okresie,
ii) wymiary urlopów pracowników w komórce organizacyjnej,
jj) zmiana wymiaru urlopu wypoczynkowego.

111. Moduł musi umożliwić generowanie raportów w różnych konfiguracjach z wszystkich elementów znajdujących się w Systemie wg stanu na określony dzień lub w przedziale czasowym, w szczególności:
a) informacje uzupełniające,
b) plany urlopów. Moduł musi umożliwić wydrukowanie stanu zatrudnienia w komórkach organizacyjnych w ujęciu etatowym i osobowym, z grupowaniem stanowisk, wg wytycznych użytkownika, z uwzględnieniem urlopów wychowawczych i bezpłatnych na dany dzień z wyliczeniem średniej z całego miesiąca.

112. Moduł musi umożliwić generowanie zestawienia zawierającego dane dotyczące stanu zatrudnienia w ramach prac interwencyjnych i robót publicznych w komórkach organizacyjnych na dany dzień lub na 1, 15 i ostatni dzień miesiąca z wyliczeniem przeciętnej z całego miesiąca.

113. Moduł musi dać możliwość wykonania raportu dla każdego pracownika -za wybrany okres od dnia, okres rozliczeniowy z bilansem przepracowanego czasu pracy uwzględniając wyjścia prywatne,

odpracowania, potrącenia za wyjścia prywatne nadgodziny, zapłatą za nadgodzin, pracą w dniu wolnym z tytułu 5 dniowego tygodnia pracy, pracy w dniu wolnym, pracy w niedzielę i święta, odebrania wolnego z tytułu niedzieli i święta, Pracy w godzinach nocnych.

114. Moduł musi umożliwić generowanie zestawienia zawierającego dane dotyczące zatrudnienia za dany dzień miesiąca lub przeciętne zatrudnienie w danym miesiącu w etatach/osobach z pracami interwencyjnymi i robotami publicznymi/bez prac interwencyjnych i robót publicznych.
115. Moduł musi umożliwić generowanie wykazu pracowników niepełnosprawnych (na dany dzień lub w przedziale czasowym) w podziale na stopnie niepełnosprawności (lub łącznie) ze wskazaniem stopnia niepełnosprawności, od kiedy pracownik posiada orzeczony stopień niepełnosprawności, od kiedy jest zaliczany do stanu zatrudnienia osób niepełnosprawnych w jednostce, jaki jest okres obowiązywania orzeczenia o stopniu niepełnosprawności, od kiedy pracownik jest zatrudniony w jednostce, ze wskazaniem wymiaru etatu pracownika oraz jego stanowiska.
116. Moduł musi umożliwić generowanie wykazu pracowników niepełnosprawnych posiadających schorzenie szczególne, które uzasadnia obniżenie wskaźnika zatrudnienia osób niepełnosprawnych w podziale na stopnie niepełnosprawności (lub łącznie).
117. Moduł musi umożliwić generowanie sprawozdania dla PFRON ze stanu zatrudnienia osób niepełnosprawnych w jednostce z wyliczeniem wskaźnika zatrudnienia osób niepełnosprawnych według średniej arytmetycznej (dodaje się stany zatrudnienia w poszczególnych dniach pracy w miesiącu łącznie z dniami wolnymi od pracy niedzielami i świętami - przyjmuje się dla tych dni stan zatrudnienia z dnia poprzedniego lub następnego, jeśli miesiąc rozpoczyna się dniem wolnym od pracy, a otrzymaną sumę dzieli się przez ilość dni kalendarzowych miesiąca sprawozdawczego) ze stanów dziennych lub na 1, 15 i ostatni dzień miesiąca w oparciu o ustawę o rehabilitacji zawodowej i zatrudnianiu osób niepełnosprawnych (art. 2, 2a, 21 ustawy).
118. Moduł musi umożliwić grupowe przeliczanie wymiaru urlopu dla pracowników.
119. Moduł musi umożliwić, w wyjątkowych przypadkach, usuwanie zatrudnienia (jeśli nie było żadnych wypłat) oraz osób (jeśli nie ma podpiętych żadnych zatrudnień, umów cywilno-prawnych, stypendiów, wynagrodzeń komisji, diet radnych.
120. Moduł musi współpracować z systemem elektronicznego rozliczenia czasu pracy (m.in. współpraca z czytnikami kart zbliżeniowych).
121. Moduł musi rozliczać czas pracy dla wybranych grup pracowników na podstawie Rejestru Czasu Pracy poprzez analizę zdarzeń na rejestratorach czasu pracy wraz z jej interpretacją i odwzorowaniem graficznym na czasie pracy danego pracownika.

PŁACE – moduł musi spełniać następujące wymagania funkcjonalne:

1. Obsługa płacowa w Module musi dotyczyć dokonywania wszelkich obliczeń dla różnych grup osób: pracownicy, osoby świadczące pracę w oparciu o umowy cywilnoprawne (umowy zlecenia i o dzieło), stypendyści, osoby otrzymujące nagrody sportowe i kultury, radni samorządowi, a także osoby biorące udział w powoływanych komisjach.
2. System musi zapewnić możliwość samodzielnego definiowania i prowadzenia rejestrów dla poszczególnych grup:
   a) pracownicy / emeryci,
   b) zatrudnieni na podstawie umów cywilnoprawnych (również rejestr zawartych umów),
   c) stypendyści,
   d) radni samorządowi,
   e) otrzymujący nagrody sportowe/kultury,

oraz:

   a) rachunków bankowych,
   b) urzędów skarbowych,
   c) potrąceń jednorazowych i stałych,
   d) komorników.

3. Kartoteka danych w Module (takich jak dane osobowe, płacowe, podatkowe, składkowe) dla wyżej wymienionych grup musi zawierać wszelkie niezbędne informacje dla prawidłowej obsługi płacowo-rozliczeniowej tych osób:
   a) PESEL/NIP,
   b) dane urzędu skarbowego,
   c) adres do celów podatkowych,

d) rodzaj kosztów uzyskania przychodów,
e) indywidualne rachunki bankowe,
f) składniki potrąceń (obowiązkowych i dobrowolnych).

4. Składniki płac/wynagrodzeń w Module dotyczyć muszą zarówno kwot ewidencjonowanych z użyciem modułu kadrowego, jak i tych, które nie są ewidencjonowane przez użytkowników modułu kadrowego. Dla prawidłowego wyliczenia list wynagrodzeń będą uwzględniane wszelkie informacje, mające wpływ na wysokość i składniki wynagrodzenia, które są zawarte w module kadrowym (na przykład rejestr nieobecności pracownika).
5. Moduł musi posiadać gotowe składniki płacowe podzielone na grupy tematyczne: płaca brutto, składniki dodatkowe, socjalne, przerwy w pracy, potrącenia dobrowolne.
6. Moduł musi automatycznie aktualizować parametry, które obowiązują w danym roku lub przedziale czasowym w celu prawidłowego naliczenia:
   - Składek na ubezpieczenie społeczne (płatnych przez pracodawcę i pracownika), zdrowotne (z uwzględnianiem sposobu wyliczenia składek ZUS, który dotyczy zarówno obowiązkowych jak i dobrowolnych ubezpieczeń) oraz składek na Fundusz Pracy.
   - Składek na Pracownicze Plany Kapitałowe.
   - Kontrola narastająco podstawy do naliczania składek emerytalnych i rentowych (zaprzestanie ich potrącania w przypadku osiągnięcia 30-krotności kwoty określonej w przepisach na dany rok, a także możliwość obsługi przypadków, kiedy osiągane są dochody z innych źródeł i stanowią również podstawę składek emerytalnych i rentowych).
   - Wynagrodzeń chorobowych i zasiłków z ubezpieczenia społecznego.
   - Podatku dochodowego od osób fizycznych z uwzględnieniem wszystkich możliwych do zastosowania ulg czy zaniechań oraz z możliwością indywidualnego zdefiniowania danych podatkowych takich, jak określenie informacji o typie kosztów uzyskania przychodu oraz o rodzaju i wysokości podatku.
7. Aktualizacja parametrów powinna dotyczyć minimalnego zakresu podanego poniżej:
   - kwota kosztów - stosunek pracy – podstawowych,
   - kwota kosztów - stosunek pracy – zwiększonych,
   - kwota rocznego ograniczenia podstawy wymiaru składek na ubezpieczenie emerytalne i rentowe,
   - kwota wolna – miesięczna,
   - kwota wolna - miesięczna w roku 2021,
   - kwota wolna naliczania składki na NFZ przy wynagrodzeniach komisji,
   - kwota wolna od podatku roczny przychód, kwota wolna od wypłat z funduszu socjalnego,
   - kwota wolna w danym roku podatkowym – cała,
   - kwota wolna zapomogi wypłaconej z ZFŚS,
   - kwota zwolniona związana z pełnieniem obowiązków społecznych i obywatelskich - art 21 ust1 pkt 16,
   - kwota zwolniona związana z pełnieniem obowiązków społecznych i obywatelskich - art 21 ust1 pkt 17,
   - liczba dni chorobowego – wynagrodzenie,
   - liczba dni chorobowego - wynagrodzenie po 50 roku życia,
   - maksymalny przychód zwolniony do ulg,
   - okres ważności podstawy chorobowego (liczony w miesiącach),
   - płaca minimalna,
   - procent podatku dla emerytów od wypłat z ZFŚS,
   - procent składki na fundusz emerytur pomostowych,
   - procent składki na fundusz gwarantowanych świadczeń pracowniczych,
   - procent składki na fundusz pracy,
   - procent składki pracownika na fundusz chorobowy,
   - procent składki pracownika na fundusz emerytalny,
   - procent składki pracownika na fundusz rentowy,
   - procent składki zakładu na fundusz emerytalny,
   - procent składki zakładu na fundusz rentowy,
   - prognozowane przeciętne wynagrodzenie miesięczne,

- próg podatkowy - dolna wartość drugiego progu podatku dochodowego od osób fizycznych,
- próg podatkowy - procent podatku dla drugiego progu podatkowego,
- próg podatkowy - procent podatku dla pierwszego progu podatkowego,
- składka na ubezpieczenie zdrowotne – cała,
- składka na ubezpieczenie zdrowotne - odbijana od podatku,
- umowa zlecenie procent kosztów – podstawowych,
- umowa zlecenie procent kosztów – zwiększonych
- wiek dla kobiet powyżej którego nie liczymy funduszu pracy,
- wiek dla mężczyzn powyżej którego nie liczymy funduszu pracy,
- wiek emerytalny kobiety,
- wiek emerytalny mężczyzny,
- wskaźnik waloryzacji świadczenia rehabilitacyjnego I kwartał,
- wskaźnik waloryzacji świadczenia rehabilitacyjnego II kwartał,
- wskaźnik waloryzacji świadczenia rehabilitacyjnego III kwartał,
- wskaźnik waloryzacji świadczenia rehabilitacyjnego IV kwartał,
- wynagrodzenie od podatku (pit 4),

8. Moduł musi posiadać możliwość naliczania różnych sposobów wynagradzania takich jak:
   - umowa o pracę,
   - umowa o dzieło,
   - umowa zlecenia,
   - wypłaty komisji działających w jednostce,
   - wypłaty ryczałtów,
   - wypłaty diet radnych
   - wypłaty stypendiów
   - wypłaty rent
9. Moduł musi posiadać możliwość tworzenia wielu rodzajów list płac takich jak:
   - lista podstawowa,
   - listy dodatkowe,
   - lista wyrównująca,
   - lista korygująca,
   - planowana trzynastka.
10. Moduł musi posiadać możliwość zbiorczego wprowadzania składników płacowych dla wybranych pracowników takich jak:
    - Diety,
    - Nagrody,
    - Ryczałty,
    - Wypłaty z Zakładowego Funduszu Socjalnego.
11. Moduł musi posiadać możliwość zadeklarowania automatycznych dodatkowych wypłat między innymi takich jak: wypłaty diet, ryczałtów, wynagrodzeń za posiedzenia komisji.
12. Moduł musi posiadać możliwość zadeklarowania automatycznych dodatkowych wypłat między innymi takich jak: wypłaty diet, ryczałtów, wynagrodzeń za posiedzenia komisji.
13. Moduł musi zawierać mechanizm automatycznego rozksięgowania listy płac na podstawie struktury klasyfikacji budżetowej prowadzonej przez jednostkę.
14. Moduł musi zawierać możliwość rozksięgowania list płac kluczem procentowym na zdefiniowane konta księgowe i konta klasyfikacji budżetowej
15. Moduł musi zawierać możliwość księgowania wypłat umów zlecenia i o dzieło w trzech trybach: księgowanie zbiorcze umów zleceń w przypadku umów masowych (np. komisje wyborcze), księgowanie zbiorcze na podstawie klucza klasyfikacji budżetowej, księgowanie pojedyncze na podstawie rachunku wystawionego przez zleceniobiorcę.
16. Moduł musi automatycznie tworzyć dekrety księgowe w systemie finansowo księgowym.
17. Moduł musi zawierać możliwość wydruku polecenia księgowania.
18. Moduł musi zawierać możliwość wydruku polecenia księgowania umów zleceń i o dzieło z dodatkową informacją dotyczącą szczegółów umowy oraz rachunku.
19. Moduł musi zapewnić możliwość wypłat z ZFŚS z uwzględnieniem pomocy rzeczowej, pieniężnej, zapomóg raz pozostałych wypłat

20. Moduł musi umożliwić automatyczne sumowanie za cały miesiąc wypłat tak aby prawidłowo naliczyć:
    - Składki ZUS,
    - Składkę zdrowotną,
    - Podatek dochodowy
21. Moduł musi zapewnić prowadzenie i generowanie kartoteki płacowej i podatkowej pracowników oraz osób obcych, w szczegółowym podziale na rodzaje osiąganych przychodów i dokonanych potrąceń w poszczególnych miesiącach danego roku.
22. Prowadzenie i drukowanie kartoteki ubezpieczeniowej (zasiłkowej) za okres, dowolnie określony przez użytkownika. Możliwość drukowania kartotek pracowników oraz osób obcych w ujęciu indywidualnym lub zbiorczym. Możliwość samodzielnego projektowania kartoteki w zależności od potrzeby użytkownika z uwzględnieniem wybranych składników, dat wypłaty, itp.
23. System musi automatycznie pobierać dane dotyczące składek i pożyczek w modułach Międzyzakładowej Pracowniczej Kasy Zapomogowo-Pożyczkowej i Zakładowego Funduszu Świadczeń Socjalnych:
    - możliwość wprowadzenia wysokości pożyczki, rat, kwoty wpisowej i składki na wkłady i definiowania harmonogramu spłat pożyczek,
    - automatyczne naliczanie pracownikowi na liście płac wymienionych potrąceń w ustalonych kwotach do czasu spłaty zadłużenia,
    - możliwość drukowania aktualnych sald pracowników w formacie indywidualnym lub zbiorczym z wyszczególnieniem wysokości wkładów i stanu zadłużenia.
    - System powinien zapewnić możliwość zmiany i korygowania kwot potrąceń przez użytkownika.
24. Moduł musi umożliwić definiowanie lub automatyczne uwzględnianie na liście płac indywidualnych składników wynagrodzenia i potrącenia (dobrowolnych i obowiązkowych), przeglądania naliczeń, potrąceń oraz rozliczonych absencji pracownika na liście płac.
25. System musi umożliwić grupowe wprowadzenie składników i potrąceń na listę płac.
26. System musi kontrolować maksymalną kwotę potrącenia, określoną w przepisach, z uwzględnieniem kwoty wolnej od potrąceń (w szczególności zajęcia komornicze).
27. System musi automatycznie wykonywać naliczenie wyrównań za okresy minione, w przypadku konieczności dokonania korekt w podziale na miesiące.
28. System po wyrównaniu wynagrodzeń powinien automatycznie wyrównać kwoty absencji, w których podstawach znalazły się okresy (miesiące) z korygowanymi wynagrodzeniami.
29. Moduł musi generować wypłaty dodatkowego wynagrodzenia rocznego „13-tki" i jednocześnie musi umożliwiać:
    a) Automatyczne określenie listy pracowników uprawnionych do otrzymania „13-tki" (którzy efektywnie przepracowali min.180 dni w poprzednim roku kalendarzowym),
    b) określenie nieobecności pracownika z podziałem na przyczyny: chorobowe, macierzyńsko-rodzicielskie, opiekuńcze, pozostałe
    c) wyszczególnienie składników wynagrodzenia, które wchodzą do podstawy „13-tki" z podziałem na miesiące
    d) automatyczne wyliczanie kwot, zmniejszających podstawę „13-tki" z tytułu różnych absencji pracownika.
    e) moduł musi zapewnić możliwość wyliczenia kwot częściowych, stanowiących podstawę „13-tki" z podziałem na odpowiednie jednostki organizacyjne czy projekty, w których dany pracownik był zatrudniony.
30. Moduł musi zapewnić możliwość wprowadzania danych dotyczących wysokości procentowej/kwotowej i wyliczeń premii regulaminowej dla wybranych pracowników.
31. Moduł musi zapewnić możliwość generowania listy wypłat za godziny nadliczbowe i za pracę w godzinach nocnych.
32. Moduł musi umożliwić automatyczne wyliczanie wartości średniej urlopowej dla pracowników, uzyskujących zmienne składniki wynagrodzenia (premie, nadgodziny, praca w godzinach nocnych).
33. Moduł musi umożliwić automatyczne obliczanie wynagrodzeń, uwzględniające okres zatrudnienia i ewentualne zmiany w wynagrodzeniu na przełomie miesiąca, wynikające ze zmiany warunków płacowych, korzystania z urlopów (np. macierzyńskich, wychowawczych, bezpłatnych) lub innych absencji.
34. Oprogramowanie musi umożliwić automatyczne rozliczanie nieobecności chorobowych pracowników i zleceniobiorców z uwzględnieniem kodu zwolnienia(zwolnienie lekarskie w okresie

ciąży, opieka, wypadek w pracy i w drodze itd.) a także z samoczynną kontrolą źródła finansowania (fundusz płac, ZUS, świadczenie rehabilitacyjne):

a) samoczynne wyliczanie podstawy wymiaru wynagrodzenia i zasiłku chorobowego z okresu 12 miesięcy uwzględniające wszystkie prawidłowe w tej kwestii składniki wynagrodzenia,

b) automatyczne wyliczanie nowej podstawy wymiaru wynagrodzenia i zasiłku chorobowego (np. przerwa trzech miesięcy kalendarzowych między nieobecnościami chorobowymi pracownika/ zleceniobiorcy, zmiany etatu od początku miesiąca, jak i w trakcie miesiąca),

c) uwzględnianie i korygowanie podstawy wymiaru wynagrodzenia i zasiłku chorobowego o utracone składniki, które przyznawane są do określonego terminu,

d) uwzględnianie w podstawie zasiłkowej właściwej części „13-tki",

e) automatyczna waloryzacja podstawy świadczenia rehabilitacyjnego w oparciu o aktualne wskaźniki.

35. Moduł musi umożliwić ewidencjonowanie absencji chorobowej pracowników - możliwość wprowadzania daty początku i końca nieobecności przez pracownika płac do celów rozliczeniowych.
36. Moduł musi umożliwić automatyczną kontrolę absencji pracowników oraz dostarczyć informacje o:
    a) wykorzystaniu i przekroczeniu 14, 33 dni wynagrodzenia za czas choroby,
    b) wykorzystaniu i przekroczeniu 14, 60 dni zasiłku opiekuńczego,
    c) upływie 182/270 dnia zasiłku chorobowego, z możliwością korekty sumy dni zasiłkowych na podstawie informacji z ZUS.
37. Moduł musi umożliwić automatyczną kontrolę naliczania składki na Fundusz Pracy:
    a) dla kobiet, przekraczających 55 rok życia i mężczyzn, przekraczających 60 rok życia, gwarantująca zaprzestanie naliczania składki w miesiącu następującym po ukończeniu powyższych lat,
    b) w okresie przebywania na urlopach macierzyńskich, ojcowskich, rodzicielskich,
    c) w okresie 36 miesięcy, po powrocie z powyższych urlopów,
    d) automatyczne wznowienie naliczania składki po upływie 36 miesięcy.
38. Moduł musi umożliwić automatyczne wyliczanie wg odpowiednich algorytmów: nagród jubileuszowych, odpraw emerytalnych, ekwiwalentów za urlop, odprawy ekonomicznej, odprawy na koniec kadencji itp.
39. Moduł musi zapewnić możliwość wykazania ilości osób zgłoszonych do ubezpieczenia wypadkowego w danym miesiącu w rozbiciu na pracowników i zleceniobiorców (IWA) oraz możliwość wykazu danych niezbędnych do deklaracji PFRON.
40. Moduł musi umożliwić Prowadzenie rejestru osób z ustalonym prawem do emerytury, którzy są jednocześnie zatrudnieni w jednostce lub wykonują pracę na podstawie umowy cywilnoprawnej na jego rzecz i późniejsza możliwość wykazania ich dochodów z rozbiciem na poszczególne rodzaje umów, składniki i potrącone składki.
41. Moduł musi zapewnić tworzenie zestawień rozrachunków z kontrahentami zewnętrznymi (ZUS, Urząd Skarbowy, komornik, bank, Ubezpieczyciel itd.) z możliwością eksportu przelewów do dowolnej bankowości elektronicznej i realizacja wpłat na poszczególne, zdefiniowane w systemie rachunki bankowe.
42. Moduł musi zapewnić prowadzenie rozliczeń wynagrodzeń z możliwością zaokrąglania obliczanych składników, w zależności od przepisów do pełnych złotówek, dziesiątek groszy lub groszy.
43. Moduł musi zapewnić ewidencje płacową świadczeń przyznanych pracownikom z Zakładowego Funduszu Świadczeń Socjalnych. Uwzględnienie potrąconego z tego tytułu podatku w rozliczeniu rocznym, uwzględnienie limitów i kwoty wolnej od podatku zgodnie z wymaganiami polskiego ustawodawstwa.
44. Moduł musi umożliwić uwzględnienie do wypłaty składników wynagrodzenia z zastosowaniem wskaźnika procentowego lub kwotowo.
45. Możliwość podziału poszczególnych składników wynagrodzenia na te, które są kwalifikowalne, zgodnie z zasadami realizowanych programów operacyjnych, UE. Możliwość określenia części wynagrodzeń na różnych listach w przypadku pracownika, zatrudnionego na kilka umów o pracę, w kilku jednostkach organizacyjnych lub w kilku projektach wg modyfikowalnej definicji użytkownika.
46. Możliwość eksportu do bankowości elektronicznej plików przelewów kwot wypłat, potrąceń i składek ZUS z przypisanych rachunków bankowych; m.in. w przypadku projektów UE.
47. Moduł musi umożliwić generowanie list płac i wszelkich zestawień wynagrodzeń dla wybranych grup:

pracownicy, osoby świadczące pracę w oparciu o umowy (umowy zlecenia i o dzieło), stypendyści, radni, osoby otrzymujące nagrody sportowe/kultury, a także osoby biorące udział w powoływanych komisjach. Zestawienia muszą być generowane ze wszystkich lub wybranych składników i potrąceń naliczonych na listach płac funduszu osobowego i bezosobowego, zbiorczo i w podziale na rozdziały, paragrafy, budżet zadaniowy, grupy pracownicze i grupy stanowisk, z możliwością sortowania tych danych wg zadanego kryterium.

48. Moduł musi umożliwić zdefiniowanie w danym miesiącu jednej listy podstawowej (dla jednostki organizacyjnej, projektu) oraz wielu list dodatkowych. Każda lista ma mieć swój niepowtarzalny numer, tytuł oraz informację, jakiego okresu dotyczy i w jakim okresie jest wypłacana oraz klasyfikację budżetową.
49. Moduł musi umożliwić wielokrotne przeliczanie całej listy płac lub w zawężeniu dla wybranych osób, do momentu generowania plików przelewu. Możliwość blokowania - oznaczania listy jako „zamkniętej" w celu uniknięcia niepożądanej edycji.
50. Moduł musi umożliwić generowanie: odcinków płacowych, potwierdzeń pobranego wynagrodzenia dla konkretnej osoby lub całej listy wypłat.
51. Moduł musi umożliwić wyszukanie każdej z list wypłat wg kryterium: nr listy, kod jednostki organizacyjnej, rodzaju (podstawowa, dodatkowa, inna wypłata), daty sporządzenia, danych osoby znajdującej się na liście, rodzaju składnika wynagrodzenia/potrącenia.
52. Moduł musi umożliwić generowanie list płac, dotyczących wynagrodzeń i oddzielnie list dodatkowych dla dowolnie definiowanych składników wynagrodzenia w ujęciu alfabetycznym osób w podziale na komórki organizacyjne.
53. Moduł musi umożliwić generowanie list wypłat zanonimizowanych bez imienia i nazwiska, tylko z numerem ewidencyjnym pracownika.
54. Każda wygenerowana w Systemie lista wypłat musi zawierać podsumowanie: System musi zapewnić możliwość generowania dowolnych zestawień z samych podsumowań list wypłat wg dowolnych kryteriów zdefiniowanych przez użytkownika.
55. Moduł musi umożliwić generowanie gotowych raportów o stanie zatrudnienia i wypłaconych wynagrodzeniach (w podziale na poszczególne składniki) oraz sprawozdań z analizami zatrudnienia i wypłaconych wynagrodzeniach dla GUS oraz ZUS, w szczególności: Z-03, Z-05, Z-06, Z-12, Z-14, z możliwością definiowania kryteriów wyboru danych.
56. Moduł musi zapewnić możliwość dowolnej edycji i korekty danych, zawartych w tych sprawozdaniach.
57. Moduł musi umożliwić sporządzanie miesięcznych i rocznych, indywidualnych oraz zbiorczych rozliczeń zaliczek podatkowych.
58. Automatyczne tworzenie formularzy PIT-11, PIT-R, PIT-IFT1, PIT-4R, PIT-8AR dla pracowników/zleceniobiorców/stypendystów/radnych/otrzymujących nagrody sportowe i kultury, według obowiązującego stanu prawnego z możliwością samodzielnej edycji i korekty brakujących/błędnych danych.
59. Moduł musi zapewnić możliwość składania deklaracji za pomocą środków komunikacji elektronicznej.
60. Moduł musi umożliwić eksport do programu PŁATNIK danych do dokumentów zgłoszeniowych do ZUS wymaganych przez ten program takich jak: ZUA, ZZA, ZIUA, ZWUA, ZCNA oraz rozliczeniowych RCA, RZA, RSA, DRA, RPA.
61. Moduł musi umożliwić sporządzanie: zaświadczeń o zatrudnieniu i zarobkach dla pracowników i zleceniobiorców, zaświadczeń ZUS Rp-7, Z-3, zaświadczeń do banku. Możliwość uzupełniania tekstu zaświadczeń o treść indywidualną, która nie występuje we wzorze.
62. Moduł musi umożliwić generowanie raportów lub zestawień z ustalaniem własnych kryteriów w formacie xls, txt i pdf z możliwością określenia zakresu dat, na które dane zestawienie ma być wykonane, możliwość definiowania raportów na stałe i zapisywania ich jako szablon i udostępniania innym użytkownikom.
63. Moduł musi umożliwić tworzenie list wypłaty ekwiwalentu za zakup i pranie odzieży i obuwia roboczego.
64. Moduł musi umożliwiać obsługę pracowników w zakresie PPK.
65. Moduł musi umożliwić wprowadzanie i modyfikację (ręczną) różnych rodzajów świadczeń socjalnych wraz z ich wysokościami dla danego roku oraz wysokości kwoty wolnej od podatku dla różnych rodzajów świadczeń i różnych grup osób uprawnionych.

66. Moduł musi umożliwić automatyczne rozliczenia świadczeń socjalnych poprzez uwzględnienie różnych form dokonywanych wypłat z ZFŚS lub potrąceń dla poszczególnych pracowników z uwzględnieniem kwoty wolnej od podatku w szczególności:
    a) wypłata pożyczki mieszkaniowej,
    b) potrącanie rat pożyczki z wynagrodzenia,
    c) wypłata zapomogi finansowej,
    d) wypłata dofinansowania do wypoczynku,
    e) wypłata dofinansowania do zajęć sportowo-rekreacyjnych,
    f) potrącenie opłaty za zajęcia sportowo-rekreacyjne z wynagrodzenia,
    g) wartość bonu towarowego,
    h) pozostałe wypłaty z funduszy ZFŚS
    i) świadczenia rzeczowe z ZFŚS
67. Moduł musi umożliwić automatyczne naliczanie dla pracownika (zatrudnionego na czas nieokreślony oraz emeryta/rencisty) wysokości rat pożyczki mieszkaniowej (utworzenie harmonogramu spłat) i naliczenie ustalonych odsetek do pierwszej raty, możliwość przesunięcia lub odroczenia terminu spłat oraz możliwość zarejestrowania indywidualnej spłaty rat pożyczki.
68. System musi automatycznie obliczać kwoty do opodatkowania, kwotę podatku i kwotę do wypłaty dla poszczególnych świadczeń z uwzględnieniem kwoty wolnej od podatku w danym roku, (automatycznie sumuje udzielone świadczenia poszczególnych pracowników i po przekroczeniu kwoty wolnej od podatku wylicza kwotę do opodatkowania).
69. Moduł musi umożliwiać prowadzenie ewidencji potrąceń dobrowolnych.
70. Moduł musi umożliwiać prowadzenie archiwum pracowników.
71. Moduł musi umożliwiać automatyczne naliczanie płac.
72. Moduł musi automatycznie kontrolować podstawę do wyliczenia składek emerytalnych i rentowych z uwzględnieniem obowiązującego w danym roku limitu.
73. Moduł musi automatycznie zaprzestać naliczania składki emerytalnej i rentowej w przypadku gdy:
74. Pracownik osiągnął roczny limit,
75. Pracodawca otrzymał informację z ZUS o zaprzestaniu naliczania składki emerytalnej i rentowej.
76. Moduł musi automatycznie kontrolować obowiązujące progi podatkowe.
77. Moduł musi umożliwić zastosowanie zwiększonego progu podatkowego w przypadku złożenia przez pracownika oświadczenia.
78. Moduł musi wygenerować i wydrukować dokument, który może zastąpić wydruk rocznego dokumentu RMUA.
79. Moduł musi automatycznie naliczać lub nie naliczać składkę na Fundusz Pracy według obowiązujących przepisów.
80. Moduł musi automatycznie naliczać składkę na Fundusz Emerytur Pomostowych dla wybranych pracowników.
81. Moduł musi zachować pełną funkcjonalność bez względu jaki status ma lista. W przypadku stanu listu ustawionej jako „zamknięta" moduł nie może ponownie przeliczyć, zmienić, zmodyfikować i usunąć danych z tej listy.
82. Konfiguracja modułu musi zapewnić prawidłowe zastosowanie ulgi podatkowej oraz kosztów podczas wypłaty listy podstawowej.
83. Moduł musi mieć możliwość wykonania następujących przelewów:
    - Przelew wynagrodzeń,
    - Przelew na podstawie rachunków umów zleceń i o dzieło,
    - Przelew diet,
    - Przelewów związany z prowadzeniem projektów UE/FE,
    - Przelew z ZFŚS,
    - Przelew ryczałtów,
    - Przelew wynagrodzeń komisji,
    - Przelew potrąceń dobrowolnych pracownika,
    - Przelew podatkowy z uwzględnieniem podatku ryczałtowego.
84. Moduł musi umożliwiać prowadzenie dowolnej ilości kont bankowych jednostki.
85. Moduł musi, w zależności od oświadczenia pracownika lub zleceniobiorcy mieć możliwość przekazania wypłat na rachunek oszczędnościowo-rozliczeniowy, kasę lub czek.
86. Moduł musi zapewnić możliwość prowadzenia więcej niż jednego konta bankowego pracownika.

87. Moduł musi zapewnić możliwość podziału wypłaty wynagrodzenia na rachunek bankowy i do kasy.
88. Moduł musi mieć możliwość skorygowania nadpłaconych składek emerytalnej i rentowej.
89. Moduł musi mieć możliwość poprowadzenia umów cywilno-prawnych dla obcokrajowców przy zastosowaniu zryczałtowanego podatku 20 procentowego.
90. Moduł musi mieć możliwość poprowadzenia umów cywilno-prawnych z kosztami autorskimi.
91. Moduł musi mieć możliwość poprowadzenia umów cywilno-prawnych o wartości nieprzekraczającej 200 zł (podatek ryczałtowy).
92. Moduł musi zapewnić swobodne definiowanie rodzajów umów cywilno-prawnych i parametrów ich naliczania.
93. Moduł musi mieć możliwość wygenerowania i wydruku formularza umowy cywilno-prawnej.
94. Moduł musi mieć możliwość wygenerowania i wydruku rachunku formularza umowy cywilno-prawnej.
95. Moduł musi mieć możliwość wygenerowania i wydruku list wypłat umów cywilno-prawnych z podziałem według klasyfikacji budżetowej.
96. Moduł musi mieć możliwość wyboru i zaznaczenia domyślnego numeru identyfikacyjnego wykorzystanego przy tworzeniu osobowych deklaracji PIT (NIP, PESEL).
97. Moduł musi zapewnić prowadzenie umów cywilno-prawnych dotyczących pracowników oraz obcych osób fizycznych.
98. Moduł musi mieć funkcję umożliwiającą poprowadzenie umów cywilno-prawnych, które będą wypłacane z częstotliwością kwartalna lub inną dowolną różniącą się od miesięcznej.
99. Moduł powinien dla zgłoszonych do składek ZUS umów cywilno-prawnych, dla których w bieżącym miesiącu nie było wypłat wygenerować odpowiednią zerową deklaracją RCA lub RZA.
100. Moduł musi w pełni zapewnić możliwość prowadzenia wypłat diet dla radnych.
101. Moduł musi być konfigurowalny w zakresie naliczenia diet w przypadku absencji radnego według obowiązującego regulaminu.
102. Moduł musi poprawnie nadzorować kwotę wolną przypisaną do działalności radnych.
103. Moduł musi zapewnić poprawne poprowadzenie wypłat dla osób, które są jednocześnie członkami wielu komisji.
104. Moduł powinien umożliwić poprowadzenie wypłat świadczenia integracyjnego.
105. Moduł powinien umożliwić poprowadzenie wypłat dla pracowników robót publicznych i interwencyjnych.
106. Moduł powinien umożliwić poprowadzenie wypłat stypendium stażowego.
107. Moduł powinien umożliwić poprowadzenie wypłat stypendium szkolnego.
108. Moduł powinien umożliwić poprowadzenie wypłat stypendium szkoleniowego.
109. Moduł powinien umożliwić poprowadzenie wypłat świadczenia osobistego na rzecz obrony.
110. Moduł powinien umożliwić przyznania zaliczki na poczet poborów.

Wymagania funkcjonalne modułu obsługi danych interesantów – jednolita wspólna kartoteka personalna systemów dziedzinowych

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł musi umożliwiać rejestrację w odrębnych kartotekach osób fizycznych i organizacji (osoby pozostałe).
2. Moduł musi pozwalać na wyszukiwanie osób/organizacji po niżej wymienionych kryteriach:
   a. dla osobach fizycznych: nazwisko, imię, nr PESEL/NIP, danych adresowych (miejscowość, ulica, numer budynku/lokalu), data urodzenia, imię ojca, matki, typ i numer dokumentu, nr tel. komórkowego, konto email, informacja o posiadaniu konta na platformie ePUAP i posiadaniu profilu zaufanego.
   b. dla organizacji pozostałych: nazwa/REGON/KRS/NIP po numerze konta bankowego, danych adresowych (miejscowość, ulica, numer budynku/lokalu), nr tel. komórkowego, konto email, informacja o posiadaniu konta na platformie ePUAP i posiadaniu profilu zaufanego
   c. dla obydwu grup: po identyfikatorze, będącym indywidualnym numerem przyporządkowanym tylko dla danej osoby.
3. Moduł musi umożliwiać wprowadzanie osób/organizacji w zakresie podstawowych danych osobowych, adresowych i dokumentów oraz możliwość dokonywania zmian/poprawek na wprowadzonych danych.
4. Dla zarejestrowanej osoby (fizycznej/pozostałej) moduł musi umożliwiać wprowadzanie:

a. kilku różnych typów adresów,
b. osób powiązanych z daną osobą (np.: dla osób fizycznych – małżonka, dla osoby pozostałej – filie, właściciele),
c. dla osób pozostałych – przynależność do grupy sprawozdawczości budżetowej – funkcja zintegrowana z aplikacją naliczającą podatek od nieruchomości w celu stworzenia zestawienie RBN,
d. dla osób pozostałych – kody PKD – funkcja zintegrowana z aplikacjami windykacyjnymi w celu stworzenia sprawozdania PKD,
e. kilku numerów kont bankowych, ze wskazaniem głównego konta w celu wystawiania przelewów w aplikacjach windykacyjnych,
f. Urzędu Skarbowego, pod który podlega osoba,
g. Zakładu Ubezpieczeń Społecznych, do którego są odprowadzane są składki.

5. Moduł musi umożliwiać przechowywanie pełnej historii osób z uwzględnieniem kiedy, jakie dane były zmieniane i przez jakiego operatora.
6. Moduł musi umożliwiać wyszukiwanie i wybór osób ze stanem archiwalnym oraz wprowadzanie zmian archiwalnych.
7. Z poziomu kartoteki osób/organizacji moduł musi zawierać informacje o „pochodzeniu danego rekordu" – czy dana organizacja/osoba pochodzi np. z importu danych, z ewidencji ludności/podmiotów gospodarczych, czy została dopisana w aplikacji.
8. Moduł musi posiadać funkcję administracyjną (dostępną tylko dla wybranych użytkowników) pozwalającą na sklejanie osób/organizacji w przypadkach gdy są kilkakrotnie wprowadzone do systemu z różnymi danymi (aktualnymi i archiwalnymi) lub pojawiły się w systemie z importu z systemów zewnętrznych. Po scaleniu dane aktualne powinny być wyświetlane w systemach dziedzinowych.
9. Moduł musi posiadać możliwość odszukania osoby, która została doklejona/ do osoby głównej, uwzględniając jej poprzednie stany.
10. Moduł musi umożliwiać tworzenie profili dla poszczególnych użytkowników aplikacji w zakresie dostępu do informacji znajdujących się w systemie dotyczących osób/organizacji – winna być możliwość - jeśli zaistnieje taka potrzeba – aby pewne informacje nie były dostępne dla danego użytkownika (np. dane adresowe, dokumenty, numer NIP/REGON/PESEL, informacje o kontach bankowych itp.).
11. Moduł musi zawierać słowniki: krajów, miejscowości, ulic, imion, adresów, rodzajów organizacji, typów dokumentów, klasyfikacji EKD/PKD, pozwalające dopisywać nowe dane i poprawiać uprzednio wprowadzone.
12. Moduł musi zawierać słowniki pieczątek/znaków graficznych wykorzystywanych w korespondencjach w zintegrowanym module podatku od nieruchomości.
13. Moduł musi posiadać funkcję importu danych z systemów zewnętrznych - Import banków z KIR (Krajowej Izby Rozliczeniowej) – po jej zastosowaniu następuje kontrola podczas wprowadzania numerów bankowych w zakresie nazwy i numeru oddziału banku.
14. Moduł musi posiadać funkcję importu danych z TERYTU systemu zewnętrznego (import danych terytorialnych dotyczących nazw miejscowości, ulic, kodów pocztowych). Na podstawie zaimportowanych słowników uzupełnia się bazę adresową w Urzędzie.
15. Kartoteka interesantów systemów dziedzinowych musi być wspólna dla wszystkich modułów oferowanego systemu oraz powinna zawierać mechanizmy jej integracji (powiązań) z kartoteką systemu EOD w szczególności w zakresie aktualizacji danych oraz wprowadzania nowych podmiotów.
16. Moduł musi współpracować z systemem eNależności oraz aplikacją mobilną za pośrednictwem serwisu komunikacyjnego w zakresie informacji danych ewidencyjnych podatników.
17. Komunikacja z systemem EOD odbywa się za pośrednictwem modułów szyny danych i brokera komunikacyjnego z wykorzystaniem udostępnionej usługi .
18. System musi zapewnić obsługę e-usług w zakresie niezbędnym do ich realizacji.

Wymagania funkcjonalne modułu e -VAT.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Portal i mechanizmy w nim zawarte mają służyć standaryzacji procedur, usprawnieniu gromadzenia danych oraz sporządzania deklaracji JPK_V7M w JST.

2. Moduł powinien być bezpośrednio powiązany z modułem obsługi deklaracji VAT *Systemu finansowo-księgowego* tzn. dane, że powinny być przetwarzane w jego obrębie.
3. Dostęp do modułu musi być możliwy poprzez bezpieczne logowanie z użyciem identyfikatora i zaszyfrowanego hasła.
4. Moduł powinien udostępniać dane zalogowanemu użytkownikowi tylko zakresie uprawnień nadanych przez administratora systemu finansowo – księgowego.
5. Moduł powinien umożliwić (jednostkom organizacyjnym JST) złożenie stosownych dokumentów niezbędnych do naliczenia zbiorczej deklaracji JPK_V7M. Te dokumenty to: deklaracja cząstkowa JPK_V7M wypełniana ręcznie (formularz dostępny w module) lub wypełniana automatycznie poprzez import z pliku oraz niezbędne załączniki: rejestry sprzedaży i zakupów w formacie pdf lub xls, zestawienie obrotów i sald, rejestr sprzedaży i zakupów w formacie JPK.
6. Moduł powinien umożliwić komunikację pomiędzy jednostką organizacyjną i JST w zakresie informowania o kompletności dostarczanej dokumentacji. Powinno się to odbywać poprzez system wielostopniowej akceptacji.
7. Moduł powinien dokonywać walidacji składanej deklaracji JPK_V7M z dołączanymi rejestrami w formacie JPK.
8. Wymiana danych powinna zostać zabezpieczona za pomocą transmisji z wykorzystaniem tokenu oraz znacznika czasu. Przy nieprawidłowych dodatkowych danych metoda nie powinna się wykonać i powinien zostać zwrócony stosowny komunikat z błędem.
9. Moduł musi funkcjonować na ogólnodostępnym serwerze internetowym i udostępniać swoją treść przy wykorzystaniu przeglądarek WWW. Budowa strony internetowej musi spełniać ogólnie przyjęte standardy kodowania WWW oraz zgodność z normą WCAG 2.
10. Wyświetlania danych dokonywane jest za pomocą przeglądarki internetowej bez konieczności instalacji dodatkowego oprogramowania, po stronie użytkownika.
11. Komunikacja z system finansowo-księgowy powinna być oparta o technologię web service, wymiana danych musi przebiegać poprzez bezpieczne, szyfrowane połączenie za pośrednictwem serwisów komunikacyjnych.
12. Moduł powinien posiadać zaimplementowane mechanizmy umożliwiające automatyzację wymiany danych pomiędzy modułem a systemem dziedzinowym. Dostępność aktualnych danych nie może dodatkowo angażować operatorów systemów dziedzinowych.
13. Udostępnianie danych użytkownika następuje po zalogowaniu się użytkownika na jego indywidualne konto.

Wymagania funkcjonalne modułu e–sprawozdawczość.

Moduł musi spełniać następujące wymagania funkcjonalne:

1. Moduł (portal) sprawczości budżetowej ma służyć ujednoliceniu i zestandaryzowaniu procedury przekazywania sprawozdań budżetowych do jednostki nadrzędnej – organu (gmina, powiat) oraz prezentacji danych tam zawartych.
2. Dostęp do modułu musi być możliwy poprzez bezpieczne logowanie z użyciem identyfikatora i zaszyfrowanego hasła oraz przez autoryzację z wykorzystaniem powszechnie dostępnego profilu zaufanego (https://pz.gov.pl).
3. Moduł powinien być powiązany być z systemem finansowo – księgowym organu a na zewnątrz udostępniony poprzez przeglądarkę internetową czyli działać w środowisku niezależnym od systemów finansowo - księgowych posiadanych przez jednostki organizacyjne.
4. Moduł powinien posiadać możliwość zaczytywania danych wygenerowanych przez systemy finansowo-księgowe jednostek organizacyjnych. Dane dołączone (po odpowiedniej weryfikacji i zatwierdzeniu) przez jednostkę organizacyjną (logowanie, uwierzytelnienie poprzez profil EPUAP) powinny być dostarczone online do jednostki nadrzędnej.
5. Moduł powinien współpracować z systemem *EOD*.
6. Moduł powinien poprzez odpowiedni system hierarchiczny powinien umożliwiać, w jednostce nadrzędnej publikację (sprawozdań jednostkowych) na zewnątrz, poprzez odpowiednio sprofilowany portal internetowy – dane powinny być udostępnione do pobrania np. w formacie pdf, xls itp.;
7. Moduł powinien posiadać możliwość składania wniosków o zmianę o dokonywanie zmian w planie dochodów i wydatków poprzez użytkowników według nadanych uprawnień.

8. Moduł powinien w zakresie analizy i kontroli system dokonywać automatycznego wyliczenia realizacji budżetu (wydatki, dochody) w podziale na jednostki organizacyjne, za wybrany okres sprawozdawczy (wartość różnicowa), tak przygotowane dane powinny zostać zadekretowane w formie polecenia księgowania w księgach rachunkowych organu.
9. Pobrane dane (sprawozdawczość jednostek) na etapie analizy powinny być również konfrontowane, w zakresie planów budżetowych, z budżetami jednostkowymi ustalonymi w księgach organu.

Wymagania funkcjonalne dla modułu dodatki mieszkaniowe

1. Moduł musi mieć możliwość prowadzenia ewidencji wnioskodawców z uwzględnieniem:
   - danych o lokalu mieszkalnym;
   - danych o osobach w rodzinie;
   - źródłach dochodu;
   - wysokości zarobków;
   - wywiadu środowiskowego.
2. Moduł musi mieć możliwość:
   - wprowadzania wniosku;
   - ustalanie dodatku;
   - wystawianie decyzji.
3. Moduł musi mieć możliwość wprowadzenia informacji o przeprowadzonym wywiadzie środowiskowym.
4. Moduł musi mieć możliwość
   - korekty wniosku;
   - korekty dodatku;
   - korekty decyzji (z uwzględnieniem przyczyny korekty).
5. Moduł musi mieć możliwość naliczania wypłat, tworzenia listy wypłat, a w konsekwencji wydruk listy, przelewów oraz list do zarządców do tej listy.
6. Moduł musi mieć możliwość wykonania oddzielnych wydruków dla list wypłat podstawowych jak i dodatkowych.
7. Moduł musi mieć możliwość eksportu danych dotyczących przelewów w celu połączenia z systemem bankowym.
8. Moduł musi mieć możliwość wygaszania dodatków z mocy ustawy.
9. Moduł musi mieć możliwość zawieszania, odwieszania wypłat dodatków.
10. Moduł musi mieć możliwość wydruku zaświadczenia o wysokości pobranych dodatków mieszkaniowych w podanym okresie.
11. Moduł musi mieć możliwość tworzenia przelewów elektronicznych z list wypłat.
12. Moduł musi mieć możliwość prowadzenia statystyki ilościowo-wartościowej dodatków.
13. Moduł musi mieć możliwość ewidencji pracowników przeprowadzających wywiady.
14. Moduł musi mieć możliwość symulacji zmiany wysokości dodatków w przypadku wprowadzenia innego ograniczenia.
15. Moduł musi mieć możliwość wprowadzenia podziału czynszu na media.
16. Moduł musi mieć możliwość kontynuacji wniosków, które wcześniej już zostały zarejestrowane i obsługiwane (ręcznie lub w innym systemie) – wprowadzenie bilansu otwarcia.
17. Moduł musi mieć możliwość dokonywania symulacji wypłat (przewidywane wydatki na dodatki mieszkaniowe na podstawie wybranego okresu Strona | 64 z zastosowaniem procentowego wskaźnika (zwiększenia, zmniejszenia).
18. Moduł musi mieć możliwość definiowania indywidualnych szablonów do wydruku decyzji.
19. Moduł musi mieć możliwość otrzymania zestawień:
    - zestawienie wypłat dodatków mieszkaniowych;
    - dodatki mieszkaniowe według zarządców;
    - statystyka dodatków mieszkaniowych.

Wymagania funkcjonalne dla modułu epracownik

1. Portal intranetowy przeznaczony jest dla użytkowników wewnętrznych systemu - pracowników oraz kadry kierowniczej.
2. Portal Pracowniczy musi zapewniać wszystkim pracownikom Zamawiającego wgląd w ich dane kadrowe i płacowe, a także dane o czasie pracy i nieobecnościach.

3. Portal musi być dostępny z poziomu ustalonego na etapie analizy adresu WWW z odpowiednim certyfikatem bezpieczeństwa SSL. Użytkownicy będą logowali się ustalonym loginem Pracownika.
4. Funkcjonalności portalu intranetowego muszą być dostępne wyłącznie dla zalogowanych użytkowników wewnętrznych portalu.
5. W obrębie Portalu Intranetowego będzie wydzielona dedykowana strefa, panel pracownika z poziomu której będą dostępne spersonalizowane informacje kadrowo-płacowe zalogowanego pracownika.
6. Portal Intranetowy musi pozwalać kadrze kierowniczej na podgląd danych swoich podwładnych zgodnie z określonymi uprawnieniami kompetencyjnymi wynikającymi z struktury organizacyjnej jednostki.
7. Portal musi umożliwiać każdemu pracownikowi (w tym przełożonemu pracownika w kontekście danych podległych pracowników) przeglądanie informacji zgromadzonych na kartotece kadrowej oraz na kartotece płacowej wraz z listami płac.
8. Panel pracownika powinien być podzielony według następujących tematów:
   - Informacja o pracowniku.
   - Zatrudnienie.
   - Wynagrodzenia.
   - Karta zadłużeń.
   - Czas pracy.
   - Urlopy pracownika
   - Wnioski pracownicze.
   - Dokumentów elektronicznych.
9. Panel kierownika powinien dodatkowo zawierać listę podległych pracowników.
10. Osoba o przypisanej roli kierownika powinna mieć informację o wymiarze oraz stanie urlopu podległych pracowników. Pozostałe dane podległych pracowników takie jak informacje związane z zawartymi umowami mogą być dostępne poprzez nadanie odpowiednich uprawnień dla konkretnego pracownika o przypisanej roli kierownika.
11. W panelu kierownika powinien znajdować się rejestr wniosków urlopowych z podziałem według odpowiednio wybranego kryterium:
    - Data wniosku,
    - Wniosek do akceptacji (zatwierdzenia),
    - Wniosek zatwierdzony,
    - Wniosek odrzucony,
    - Odwołanie urlopu przez pracownika,
    - Odwołanie urlopu przez pracodawcę (kierownika),
    - Nazwiska pracownika,
12. W panelu kierownika musi być funkcjonalność pozwalająca na pracę z wnioskami urlopowymi, taka jak:
    - Szczegółowy podgląd wniosku,
    - Akceptacja wniosku,
    - Odrzucenie wniosku,
    - Anulowanie urlopu,
    - Przekazanie wniosku dalej (do innego kierownika),
    - Wydruk wniosku w postaci pliku PDF,
    - Wysłanie informacji a stanie wniosku urlopowego do pracownika.
13. Portal pracowniczy w zakresie danych pracownika musi zawierać informacje:
    - Nazwisko, Imię,
    - Drugie imię,
    - Nr Pesel,
    - Daty Urodzenia,
    - Miejsca Urodzenia,
    - Płeć,
    - Stanu cywilnego,
    - Nazwisko rodowe,
    - Imię ojca,
    - Imię matki,

- Obywatelstwo,
- Numer NIP,
- Numer dowodu osobistego i przez kogo został wydany oraz data ważności,
- Wykształcenie,
- Tytuł naukowy,
- Urząd skarbowy,
- Kod oddziału NFZ,
- Informację o zgodzie lub sprzeciwie o przetwarzaniu danych w celach marketingowych oraz ich przekazywania innym administratorom danych,
- Adres zamieszkania,
- Adres zameldowania,
- Adres do korespondencji,
- Pozostałych danych do kontaktu,
- Informacja o przyznanych oznaczeniach,
- Informacja o przynależnościach do organizacji związkowych,
- Dane osoby, którą należy powiadomić w razie wypadku,
- Dane o stosunku do służby wojskowej,
- Dane dotyczące ukończone szkół, nazwa szkoły, typ szkoły,
- Zawód wyuczony,
- Okres pobierania nauki,
- Dane związane z poprzednim zatrudnieniem, a w szczególności takie jak: Nazwa zakładu pracy, Stanowisko, Daty zatrudnienia, Wymiar etatu, Sposób rozwiązania umowy, Informacji o udzielonych urlopach bezpłatnych.

14. Moduł musi wyświetlić na podstawie wprowadzonych poprzednich okresów zatrudnienia informację ile trwało to zatrudnienie w latach, miesiącach i dniach z uwzględnieniem przerw związanych , z udzielonym urlopem bezpłatnym.
15. Informację o odbytych szkoleniach.
16. Informację o nabytych kwalifikacjach,
17. Portal pracowniczy w zakresie informacji o zatrudnieniu powinien zawierać:
    a) Umowy zawarte z pracownikiem: wykaz zawartych z pracownikiem umów, rodzaj umowy, wymiar etatu, składniki wynagrodzenia a w szczególności:
        - Rodzaj umowy,
        - Data umowy,
        - Sposób rozwiązania umowy,
        - Przypisanie do komórki organizacyjnej,
        - Zajmowane stanowisko służbowe,
        - Pełniona funkcja służbowa,
        - Przynależność do grupy zatrudnionych,
        - Wymiar etatu,
        - Typ obowiązującej pracownika stawki (wynagrodzenie miesięczne, wynagrodzenie godzinowe),
        - Składniki wynagrodzenia, Wartość procentowa i kwotowa wysługi lat (dodatek stażowy).

    b) Badania lekarskie: informacja o rodzaju badań lekarskich wraz z czasookresem ich obowiązywania,
    c) Szkolenia BHP: informacja o rodzaju szkoleń BHP w raz z czasookresem ich obowiązywania,
    d) Orzeczenia o niepełnosprawności: informacja wraz z czasookresem, na który jest wydane orzeczenie o niepełnosprawności, wraz z informacją o stopniu niepełnosprawności,
    e) Szkolenia/Kursy pracownicze: informacja o odbytych szkoleniach oraz kursach.
    f) Informacje o wynagrodzeniach a w szczególności:
        - Wynagrodzenia: informacja o zrealizowanych listach płac wraz z wykazem analitycznym składników płacowych, informacji o naliczonych składkach społecznych i zdrowotnych, naliczonym podatku, zastosowanych kosztach uzyskania przychodu oraz kwoty wolnej, zastosowanych potrąceniach od netto, naliczonym wynagrodzeniu chorobowym oraz wypłat zasiłków, informacja o wynagrodzeniach powinna zostać

wyświetlona z uwzględnieniem okresu miesięcznego oraz rocznego, w którym została wypłacona.
- Pracownik musi mieć możliwość wygenerowania na podstawie wybranej listy płac wydruku w formie paska wynagrodzeń w formacie PDF.
- Świadczenia socjalne: informacja analityczna o przyznanych świadczeniach socjalnych.
- Informacja PIT: wykaz deklaracji PIT sporządzonych i wysłanych do Urzędu Skarbowego, pracownik powinien mieć możliwość przeglądnąć wybraną deklarację oraz ją wydrukować.

18. Portal powinien zawierać podmoduł karta zadłużeń prezentujący wykaz systemów pożyczkowych (KZP, ZFŚS), do których przystąpił pracownik wraz z wykazem zadłużeń, stanu wkładów członkowskich, potrącanych składek oraz potrącanej spłaty na rzecz zadłużenia.
19. Portal powinien umożliwiać prezentację czasu pracy a w szczególności:
    a) Czas pracy: informacja o czasie pracy danego pracownika, kalendarz czasu pracy wraz z odnotowaniem wszystkich zdarzeń i absencji pracowniczych.
    b) Urlopy: wykaz urlopu bieżącego, wykaz urlopu zaległego, wykaz urlopu na żądanie, wykaz urlopu szkoleniowego, wykaz dni lub godzin opieki nad zdrowym dzieckiem, wykaz urlopów okolicznościowych, wykaz urlopu szkoleniowego, informacja o urlopie wykorzystanym oraz pozostałym do wykorzystania w zależności od rodzaju urlopu.
    c) Wnioski urlopowe - rejestr wniosków urlopowych z podziałem według odpowiednio wybranego kryterium:
        - Data wniosku,
        - Wniosek do akceptacji (zatwierdzenia),
        - Wniosek zatwierdzony,
        - Wniosek odrzucony,
        - Odwołanie urlopu przez pracownika,
        - Odwołanie urlopu przez pracodawcę (kierownika),
        - Rodzaj urlopu (wypoczynkowy, okolicznościowy, szkolny, odbiór dni wolnych lub niestandardowych, które zostały zarejestrowane w programie kadrowo-płacowym).
    d) Kreator wniosku urlopowego wraz z możliwością jego uzupełnienia, określenia rodzaju urlop, czasu trwania oraz przesłania do akceptacji swojemu kierownikowi.
    e) Odwołanie zaakceptowanego wniosku urlopowego.
    f) Anulowanie wniosku urlopowego, który został przesłany do kierownika a nie został jeszcze przez niego zaakceptowany
    g) Moduł powinien pracować na aktualnych danych kadrowo-płacowych. W celu uniknięcia wyświetlenia mylnych informacji z danych które są w edycji, modyfikacji, symulacji wynagrodzeń.
    h) Pracownicy jednostki powinni mieć możliwość podglądu m.in. wykorzystanego i planowanego urlopu, odbytych szkoleń,
20. Portal pracowniczy umożliwia pracownikowi na podgląd oraz wydruk dokumentów elektronicznych w postaci PDF z podziałem na:
    a) Załączniki z aktówki.
    b) PIT-y.
    c) Wydruki płacowe.
21. Portal pracowniczy umożliwia użytkownikom na składanie wniosków:
    a) Wniosek urlopowy z wyszczególnieniem typu urlopu (wypoczynkowy, na żądanie, okolicznościowy itp.)
    b) Wniosek informujący o braku karty RCP.
    c) Wniosek o wyjście prywatne.
    d) Wniosek o delegację.
    e) Wniosek szkoleniowy.
    f) Wniosek związany z nadgodzinami.
22. Portal pracowniczy w zakresie powiadomień umożliwia:
    a) Wyświetla kierownikowi informację o otrzymanych wnioskach
    b) Informuje użytkownika o zmianie statusu jego wniosku
    c) Umożliwia przejście do widoku wniosku poprzez powiadomienie

d) Umożliwia przechowywanie powiadomień oraz ich usuwanie

23. Portal pracowniczy umożliwia użytkownikom zmianę hasła. Jeśli hasło użytkownika zostało wygenerowane pierwszy raz lub zresetowane w programie kadrowo-płacowym, panel do zmiany hasła zostanie wyświetlony automatycznie po zalogowaniu.
24. Panel administratora umożliwia :
    a) Wyświetlenie stanu oraz ustawień połączenia z serwisami wraz z możliwością ich ponownego przeładowania.
    b) Parametryzację widoku zakładek (możliwość zarządzania widocznością zakładek oraz poszczególnych wniosków).
    c) Zarządzanie polityką haseł (ustawienie długości hasła, jakie parametry będą obowiązywać przy zmianie hasła).
    d) Możliwość przywrócenia domyślnych ustawień.
    e) Wybór sposobu logowania (logowanie domenowe).
    f) Zarządzanie rolami pracowników w strukturach oraz płatnikach (widoczność umów oraz wynagrodzeń).
25. Moduł internetowa informacja kadrowo płacowa pracownika musi mieć możliwość odnotowania przez pracownika w swoim harmonogramie pracy zrealizowanych w ramach czynności służbowych w określonym czasokresie.
26. Wprowadzona ewidencja zrealizowanych czynności służbowych musi być widoczna dla pracownika oraz jego przełożonego – użytkownika z uprawnieniami kierownika.
27. Wizualizacja wykonanych prac (czynności służbowych) powinna być dostępna na kalendarzu w układzie miesięcznym, tygodniowym i dziennym w odpowiednio dobranej szczegółowości prezentacji danych.
28. Ewidencja powinna umożliwić odnotowanie czasu poświęconego na dane zadanie, tematyki prac oraz możliwość dodatkowego załączenia dokumentów elektronicznych – zestawień szczegółowych w zakresie realizowanych prac w obrębie danego zadania (czynności).
29. Czynności służbowe powinny być typizowane w ramach słownika konfigurowanego w module kadrowym przez osobę do tego upoważnioną.
30. Słownik czynności służbowych musi być dostępny w module internetowa informacja kadrowo płacowa pracownika w module „Zrealizowane czynności służbowe”.
31. System powinien weryfikować w obrębie modułu kadrowego czas pracy pracownika i w takim zakresie kontrolować wprowadzanie czynności służbowych. W przypadku niezgodności danych z ewidencją kadrową system powinien o tym informować użytkownika i wyróżniać takie czynności celem ich weryfikacji przez przełożonego.
32. System powinien zapewnić raporty prac zarówno w odniesieniu do pojedynczego pracownika jak i grupy pracowników. Raporty powinny umożliwiać zestawienia syntetyczne jak i analityczne w odniesieni do wybranego pracownika.

Wymagania funkcjonalne modułu rejestracja czasu pracy (rcp).

1. Moduł musi umożliwiać odczyt zdarzeń dla wejścia, wyjścia, wyjścia służbowego i wejścia służbowego za pomocą dedykowanego rejestratora czasu pracy.
2. Moduł musi umożliwiać identyfikację rozpoczęcia i zakończenie pracy oraz wejścia i wyjścia prywatne/służbowe za pośrednictwem czytników kart elektronicznych. W związku z tym System musi pobierać te dane do bazy danych i prezentować je w ewidencji czasu pracy pracownika.
3. Moduł powinien umożliwiać rozliczanie czasu pracy na podstawie ustalonych harmonogramów przypisanych pracownikom lub na podstawie ruchomego rozkładu czasu pracy umożliwiającego rozpoczęcie pracy w określonych godzinach np. pomiędzy godz. 7.00 a 8.00 (możliwość dowolnej modyfikacji) i obowiązkiem świadczenia pracy przez kolejne 8 godzin (możliwość dowolnej modyfikacji).
4. Rozliczanie czasu pracy na podstawie zarejestrowanych zdarzeń - różnych statusów RCP:
    - Wejście,
    - Wyjście,
    - Wyjście służbowe,
    - Wejście służbowe.
5. Moduł powinien umożliwiać rejestracje spóźnienia w przypadku odbicia się na czytniku w dniu roboczym po określonej godzinie (np. po 7:45 - wyjście prywatne trwające od godz. 7:30 do godziny

odbicia się na czytniku danego dnia - w przypadku ściśle określonych godzin rozpoczęcia i zakończenia pracy).

6. Moduł musi umożliwić wydruk kart ewidencji czasu pracy miesięcznych / za okres rozliczeniowy/rocznych które będą zawierały informacje zgodnie z obowiązującymi przepisami prawa.
7. W Module musi być możliwość ewidencjonowania:
    - nadgodzin,
    - odebrania nadgodzin,
    - zapłaty za godziny nadliczbowe,
    - pracy w dniu wolnym z tytułu pięciodniowego tygodnia pracy,
    - odebrania dnia wolnego z tytułu 5 dniowego dnia pracy,
    - pracy w niedzielę i święta,
    - odebranie dnia za pracę w niedzielę i święta,
    - wyjść prywatnym,
    - odrobienie wyjść prywatnych,
    - potrącenie wynagrodzenia z tytułu wyjścia prywatnego,
    - pracy w godzinach nocnych.
8. Rejestrator czasu pracy musi umożliwiać odczyt oraz wysyłkę zdarzeń do programu kadrowego.
9. Rejestrator czasu pracy musi przechowywać zdarzenia w pamięci nawet po zaniku zasilania.
10. Rejestrator musi umożliwiać zablokowanie odczytu niezapisanych kart w celu eliminacji niepożądanych zdarzeń oraz wyświetlić odpowiedni komunikat przy próbie zbliżenia karty której brak w systemie.
11. System musi umożliwiać dodanie kilku rejestratorów czasu pracy oraz pobierania z nich danych.
12. Moduł musi umożliwiać zapisywanie zdarzeń w pliku tekstowym który później jest odczytywany i analizowany przez program kadrowy.
13. Rejestrator musi współpracować z kartami zbliżeniowymi działającymi w jednej z technologii: Mifare albo Unique.
14. Moduł musi przypisywać odpowiednie zdarzenia wraz z godziną do pracownika.
15. Moduł musi umożliwiać ręczną korektę wprowadzonych zdarzeń.
16. Moduł musi umożliwiać podłączenie rejestratora czasu pracy do sieci lokalnej poprzez przypisanie mu odpowiedniego adresu IP.
17. Moduł musi zapewniać automatyczną interpretację zdarzeń wejścia i wyjścia w celu odpowiedniego obliczania godzin obecności pracownika w pracy oraz naliczenie na ich podstawie typów obecności/nieobecności w programie kadrowym.
18. Moduł musi umożliwiać powiązanie pracownika z kartą współpracującą z rejestratorem czasu pracy.
19. System powinien umożliwiać automatyczne pobieranie zdarzeń z rejestratorów czasu pracy przy pomocy dedykowanego narzędzia
20. Moduł musi umożliwiać dostosowanie pracownika na rozliczanie czasu pracy wg zdarzeń z rejestratora czasu pracy.
21. Moduł musi umożliwiać przeniesienie danych z rejestratora czasu pracy na harmonogram pracy osób zatrudnionych.
22. Moduł musi umożliwiać wydruk harmonogramu czasu pracy z uwzględnieniem odczytanych zdarzeń wejścia i wyjścia.
23. Moduł powinien obsługiwać wnioski zatwierdzone w Portalu. Użytkownik systemu musi mieć możliwość automatycznego przeniesienia wniosków urlopowych, wniosków o wyjście prywatne, wniosku o opiekę nad zdrowym dzieckiem na czas pracy danego pracownika.

Wymagania funkcjonalne modułu komunikacyjnego petent-urząd

1. Moduł komunikacyjny powinien umożliwić udział mieszkańcom w zaplanowanym przez urząd e-spotkaniu w formie wideokonferencji.
2. Moduł komunikacyjny powinien umożliwić umówienie spotkania osobistego petenta w urzędzie.
3. Moduł komunikacyjny powinien umożliwić umówienie e-spotkania (spotkanie online) z wybranym pracownikiem urzędu wykorzystując jedną z poniższych metod:
    - połączenia audio,
    - połączenia wideo.

4. Moduł komunikacyjny musi mieć wydzieloną strefę dla petenta (Panel petenta) widoczną w elektronicznym biurze obsługi mieszkańca umożliwiającą:
    a) Dołączenie do zaplanowanego e-spotkania w formie wideokonferencji.
    b) Umówienia spotkania osobistego w urzędzie w wybranym przez siebie dostępnym wolnym terminie i godzinie.
    c) Umówienia e-spotkania (spotkanie online) w urzędzie w wybranym przez siebie dostępnym wolnym terminie i godzinie.
    d) Panel petenta musi wyświetlać, które terminy oraz godziny są wolne, możliwe do zarezerwowania na spotkanie osobiste lub e-spotkani przez petenta.
    e) Panel petenta powinien umożliwić przed dokonaniem rezerwacji terminu wybranie referatu lub zakresu sprawy, którą chce załatwić mieszkaniec.
5. Moduł komunikacyjny musi mieć możliwość planowania i inicjowania spotkań z mieszkańcami w formie wideokonferencji.
6. Informacje o spotkaniach z mieszkańcami w postaci wideokonferencji muszą być umieszczane w elektronicznym biurze obsługi mieszkańca.
7. Udział mieszkańca w zaplanowanych wideokonferencjach musi nastąpić poprzez elektroniczne biuro obsługi mieszkańca.
8. Moduł komunikacyjny musi mieć wydzieloną strefę dla pracowników urzędu (Panel pracownika) widoczną w elektronicznej informacji kadrowo płacowej pracownika
9. Panel pracownika musi umożliwiać:
    a) Planowania pracy pracowników urzędu obsługujących petentów w zakresie wydzielenia z ich czasu pracy określonych dni oraz godzin, w których będzie możliwość spotkania osobistego lub e-spotkania umówionego wcześniej przez moduł komunikacyjny.
    b) Terminy, daty oraz godziny pracy referatu lub pracownika muszą być widoczne w Panelu petenta tak aby była możliwa rezerwacja terminu spotkania osobistego lub e-spotkania.
    c) Panel pracownika musi w sposób jednoznaczny określać czy wybrany termin spotkania osobistego czy e-spotkania przez petenta jest wolny.
    d) Panel pracownika modułu komunikacyjnego musi współpracować z modułami HR w zakresie czasu pracy pracownika w taki sposób aby uniemożliwić wyświetlenie terminu wolnego w Panelu petenta wtedy gdy dany pracownik jest nieobecny.

7.2. eBOM - elektroniczne Biuro Obsługi Mieszkańca– licencja szt. 1 – wymagania minimalne

Wymagania funkcjonalne dla centralnego portalu elektronicznego biura obsługi mieszkańca.

Centralna platforma eBOM powinna zapewnić mieszkańcom dostęp do e-Usług oferowanych w ramach wdrożonego jednolitego systemu ze szczególnym uwzględnieniem obsługi systemów odpowiedzialnych za naliczanie opłat i podatków wraz z możliwością bezpośredniego dokonywaniem płatności elektronicznych. Platforma ta powinna też zapewnić komunikację z mieszkańcami za pośrednictwem wiadomości SMS, e-mail i komunikatów PUSH na aplikację mobilną. Dostarczone rozwiązanie musi być w pełni kompatybilne z użytkowanymi systemami dziedzinowymi wdrażanym w ramach niniejszego postępowania a komunikacja musi być realizowana online za pośrednictwem systemów serwisów komunikacyjnych zainstalowanych na infrastrukturze zamawiającego. Platforma eBOM powinna być dostępna zarówno dla użytkowników zalogowanych (uwierzytelnionych za pośrednictwem Krajowego Węzła Identyfikacji Elektronicznej lub wewnętrznych danych dostępowych – login i hasło wraz z odpowiednią procedurą uwierzytelnienia dla jednostek prawnych) jak i dla osób niezalogowanych w zakresie informacyjnym o możliwości realizacji wybranych e-usług z opisami procedur oraz możliwością pobrania odpowiednich formularzy – wzorów dokumentów itp., oraz dostępem do treści ogólnodostępnych. Platforma powinna mieć odpowiednią budowę z uwzględnionym podziałem na strefy (moduły) merytoryczne odpowiedzialne za poszczególne zadania. Oferowane rozwiązanie powinno być zgodne z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (dalej: ustawa o dostępności cyfrowej). Nadrzędnym celem uruchomienia

portalu eBOM jest zebranie w jednym miejscu informacji obejmującej różne aspekty działalności Urzędu. Aby informacja ta była łatwo dostępna, treści publikowane w portalu zostaną podzielone tematyczne. Karty e-usługi powinny być pogrupowane wg. wydziałów wraz z możliwością wyszukiwania ich za pomocą haseł tematycznych. Portal eBOM powinien posiadać wspólny interfejs graficzny i udostępnione będą w nim poszczególne moduły związane ze świadczeniem e-usług. Powinien być oparty o dedykowany system zarządzania treścią, który pozwoli na profilowanie przekazywanych informacji. Platforma ta, będąca centrum e-usług publicznych, będzie udostępniała następujące grupy funkcjonalności:

- moduł weryfikacji tożsamości petenta z wykorzystaniem Krajowego Węzła Identyfikacji Elektronicznych
- modułu odpowiedzialne za realizację płatności zintegrowane z systemem dziedzinowym urzędu
- moduł do publikacji Informacji publicznej,
- harmonogramy (kalendarze)
- moduł powiadomień
- katalogu usług publicznych (karty usług, integracja ePUAP i e-Doręczenia),

System powinien umożliwić także publikowanie danych otwartych w ogólnodostępnej części wg. podziałów na grupy danych z możliwością obsługi różnych formatów danych do pobrania oraz wywoływania adresów serwisów zawierających odpowiednie informacje
Przy projektowaniu portalu wykonawca powinien zapewnić zgodność z wymogami WCAG 2.1. W tym zakresie w szczególności należy uwzględnić poniższe kryteria stosowane przy prezentacji danych w portalu:

Solidność / kompatybilność
Responsywność i dostosowane do odczytu również na specjalnych readerach stosowanych m.in. przez osoby niedowidzące. Można je z łatwością odczytać na smartfonie w układzie poziomym i pionowym, a także przy wykorzystaniu różnych przeglądarek i systemów operacyjnych.
Zrozumiałość
Zrozumiałość zarówno w aspekcie treści, jak i formy. W tym kontekście istotne są:

- stosowanie jasnego, przejrzystego języka,
- przewidywalność treści – konsekwencja nawigacji oraz identyfikacji poszczególnych sekcji,
- wolność od błędów i jasne ich komunikowanie przez system.

Funkcjonalność
Rozumiana m.in. jako:

- możliwość łatwego sterowania stroną z poziomu klawiatury (bez myszki), a więc m.in. obsługa jednoklawiszowych skrótów i brak „pułapek klawiaturowych";
- zapewnienie użytkownikowi wystarczającego czasu na zapoznanie się z treścią i skorzystanie z niej (to np. możliwość wyłączenia/dostosowania limitów czasowych wyświetlanych elementów typu slidery);
- dostosowanie sposobu wyświetlania treści do potrzeb osób z padaczką (brak migających, jaskrawych elementów),
- szerokie możliwości nawigacji, w tym możliwość pominięcia bloków, dostęp do podstron wieloma drogami, dodanie metadanych,
- dostęp do wszystkich metod obsługi – np. udostępnienie gestów jednopunktowych dla funkcji standardowo wykorzystujących gesty wielopunktowe, możliwość rezygnacji ze wskazania i wyłączenie dodatkowych funkcji typu uruchamianie określonych akcji przez potrząśnięcie urządzeniem.

Postrzegalność
Przedstawianie treści w sposób postrzegalny dla zmysłów odbiorców, także tych ze specjalnymi potrzebami. W tym kontekście mowa m.in. o:

- stworzeniu tekstowej alternatywy dla wszystkich nietekstowych elementów, np. grafik,
- zapewnieniu dostępu do multimediów w wersjach przyjaznych dla niesłyszących czy niewidomych,

- możliwość adaptacji (np. możliwość odczytania treści w formie audio, zrozumiała kolejność sekcji, opcje wyświetlania serwisu w wersji poziomej i pionowej),
- rozróżnialność – to m.in. możliwość ustawienia wysokiego kontrastu, wielkości liter oraz odstępów między literami, wyrazami i wierszami.

Wymagania ogólne dotyczące instalacji i administracji platformę eBOK

Platforma eBOM powinna być dostarczona przez Wykonawcę i udostępniana przez niego w okresie gwarancji na infrastrukturze spełniającej warunki zarówno pod względem bezpieczeństwa danych jak i zapewnienia odpowiedniego poziomu SLA na poziomie minimum 99,95%. W zakresie wsparcia Wykonawca powinien zapewnić system zgłaszania awarii oraz możliwość wsparcia administratora lokalnego przez pracowników wykonawcy odpowiedzialnymi za prawidłowe funkcjonowanie platformy eBOM. Dla sytuacji awaryjnych (awarie krytyczne) wymagany jest dostęp do wsparcia po stronie Wykonawcy w trybie **24/7** w ramach udzielonej gwarancji. Pozostałe zgłoszenia dotyczące funkcjonowania portalu powinny być realizowane w godzinach pracy zamawiającego. Wykonawca nie będzie odpowiadał za przerwy w funkcjonowaniu platformy eBOM wynikające z awarii platform centralnych zintegrowanych z portalem oraz za przerwy związane z udostępnianiem danych przez serwisy komunikacyjne zainstalowane po stronie zamawiającego jeżeli przyczyna ich awarii leży po jego stronie.

1. Portal eBOM zostanie zrealizowany jako serwis WWW dostępny publicznie w sieci Internet z wydzieleniem części ogólnie dostępnej dla użytkowników anonimowych oraz części dostępnej po uwierzytelnieniu użytkownika. Formatowanie publikowanych treści ma następować w oparciu o zdefiniowane szablony, zapewniające spójną prezentację informacji na całej platformie.
2. Dostarczane rozwiązanie będzie zgodne z obowiązującym stanem prawnym, przepisami prawnymi regulującymi działalność samorządu we wszystkich dziedzinach jego funkcjonowania. W szczególności należy podkreślić zgodność z Krajowymi Ramami Interoperacyjności. Dostarczony system powinien mieć możliwość obsługi za pomocą najpopularniejszych przeglądarek internetowych a także za pomocą urządzeń mobilnych. EBOM musi się charakteryzować wysoką dostępnością i być zgodny ze standardami dostępności treści internetowych WCAG 2.1. Portal będzie w sposób intuicyjny kierował użytkownikami dając możliwość przechodzenia od ogółu do szczegółu.
3. W zakresie *architektury portalu:*
   a) System musi być zaprojektowany w modelu trójwarstwowym:
      - warstwa danych,
      - warstwa aplikacji,
      - warstwa prezentacji - przeglądarka internetowa - za pośrednictwem której następuje właściwa obsługa systemu przez użytkownika końcowego.

   b) System powinien umożliwiać pracę na bazie typu Open Source bądź na komercyjnym systemie bazodanowym.
   c) System w warstwie serwera aplikacji i bazy danych powinien mieć możliwość uruchomienia w środowiskach opartych na systemach operacyjnych Linux lub równoważnych lub w środowiskach opartych na systemie Windows lub równoważnych.
   d) System w warstwie klienckiej powinien poprawnie działać w różnych środowiskach z popularnymi przeglądarkami. System powinien realizować wszystkie czynności przez przeglądarkę internetową.
   e) System musi pracować w wersji sieciowej z wykorzystaniem protokołu TCP/IP oraz być w pełni kompatybilny z sieciami TCP/IP. Architektura systemu powinna umożliwiać pracę jedno i wielostanowiskową, zapewniać jednokrotne wprowadzanie danych tak, aby były one dostępne dla wszystkich użytkowników.
   f) W przypadku gdy system do pracy wykorzystuje silnik bazy danych, baza taka musi być kompatybilna z systemem operacyjnym i musi istnieć możliwość jej instalacji i pracy na zasadach określonych jak dla systemu.
   g) W zakresie wydruków musi wykorzystywać funkcjonalność systemu operacyjnego i umożliwiać wydruk na dowolnej drukarce zainstalowanej i obsługiwanej w systemie operacyjnym, na którym zostanie uruchomione oprogramowanie (drukarki lokalne, drukarki sieciowe).

h) Interfejs użytkownika (w tym administratora) powinien być w całości polskojęzyczny.
i) System musi zapewniać bezpieczeństwo danych zarówno na poziomie danych wrażliwych jak i komunikacji sieciowej przy zastosowaniu bezpiecznych protokołów sieciowych.
j) System powinien być skalowalny, zwiększenie zasobów obsługujących warstwę aplikacyjną, zwiększenie zasobów obsługujących warstwę bazy danych.

Uwierzytelnienie i administrowanie kontami

4. System musi umożliwiać użytkownikom portalu zakładania na nim indywidualnych kont. Przy rejestracji konta wymagane powinno być podanie adresu e-mail (będącego jednocześnie loginem do konta) a jego weryfikacja będzie potwierdzona przez przesłanie na wskazany adres do korespondencji wiadomości e-mail z linkiem do autoryzacji konta.
5. Założenie konta powinno być powiązane z akceptacją regulaminu portalu oraz zapoznania się z polityką przetwarzania danych osobowych.
6. Konta użytkowników powinny być podzielone na osoby fizyczne i prawne.
7. System musi umożliwiać zakładanie kont dla osób prawnych. Weryfikacja takiego konta odbywać się będzie przez administratora systemu na podstawie przesłanego formularza zgłoszenia podpisanego przez osobę uprawnioną do reprezentowania danego podmiotu lub alternatywnie przez podanie danych unikalnych dla danego podmiotu a zapewniających wiarygodną autoryzację (unikalne dane charakterystyczne z systemu dziedzinowego).
8. Przy założeniu konta podmiotu (osoby prawnej - firmy) wymagane będzie podanie numeru NIP na podstawie którego, po weryfikacji konta będą na nim udostępniane dane z systemu bilingowego zakładu w zakresie tego podmiotu.
9. Przy zakładaniu konta wymagane będzie na etapie rejestracji podanie hasła którego odpowiednia siła będzie weryfikowana przez portal eBOM. Formularz rejestracji powinien wymagać także dwukrotne wprowadzenie hasła i przeprowadzić weryfikację poprawności wprowadzanych danych na etapie zakładania konta.
10. W obrębie zarejestrowanych kont osób fizycznych system powinien zapewnić wiarygodne uwierzytelnienie mieszkańca z wykorzystaniem Krajowego Węzła Identyfikacji Elektronicznej i powiązanie logowania do konta użytkownika z mechanizmem uwierzytelnienia opartego o to rozwiązanie. Konta uwierzytelnione tą metodą należy traktować jako uprawnione do przeglądania danych z systemów dziedzinowych w zakresie osoby zalogowanej. Dane te będą udostępniane na podstawie numeru PESEL pozyskanego z Krajowego Węzła Identyfikacji Elektronicznej.
11. System powinien też umożliwić uwierzytelnienie konta na podstawie danych charakterystycznych osoby podanych przez niego w procesie zakładania konta. Zakres danych do weryfikacji będzie uzgodniony z Zamawiającym na etapie wdrożenia systemu i musi on objąć dane odbiorcy ewidencjonowane w systemie dziedzinowym (np.: nr PESEL, nr umowy, nr kartoteki odbiorcy wielkość podatku itp.). Wymagane będzie podanie co najmniej dwóch danych celem weryfikacji klienta.
12. Kolejne logowanie do konta osoby fizycznej uwierzytelnionego i powiązanego z tożsamością weryfikowaną za pośrednictwem Krajowego Węzła Identyfikacji Elektronicznej powinno być możliwe także w oparciu o ten mechanizm bez konieczności podawania hasła użytego przy rejestracji konta.
13. Konto użytkownika powinno posiadać możliwość podania numeru telefonu komórkowego celem jego wykorzystania go w module powiadomień. Podanie numeru telefonu komórkowego nie powinno być wymagane a jego zatwierdzenie musi być potwierdzone jednorazowym kodem otrzymanym za pośrednictwem wiadomość SMS na wskazany numer.
14. Konto użytkownika powinno być wspólne dla platformy eBOM jak i dla dedykowanej aplikacji mobilnej.
15. Użytkownik w obrębie konfiguracji konta powinien mieć możliwość ustawienia własnych preferencji w zakresie kolorystyki portalu, wielkości czcionki, kontrastowości oraz tematów otrzymywanych powiadomień oraz subskrybowania kalendarzy (harmonogramów).
16. System powinien posiadać mechanizm rejestracji i wyświetlania logów z pracy użytkownika.
17. Usuwanie konta użytkownika powinno być potwierdzone przez wysłanie na wskazany adres e-mail linku do dezaktywacyjnym wybranego konta.
18. Platforma eBOM musi spełniać wszelkie wymogi związane z ochroną danych osobowych,

Obsługa zobowiązań i realizacja płatności (strefa zalogowana) - integracja z centralna platformą ePłatność (PeP)

19. System musi umożliwiać zalogowanemu i uwierzytelnionemu użytkownikowi dostęp bezpośredni do danych z systemu naliczającego dany podatek lub opłatę z możliwością dokonywania zapłat za pośrednictwem systemu płatności elektronicznych, również na urządzeniach mobilnych. W szczególności integracja musi objąć moduły systemu bilingowego w zakresie modułów rozliczających opłaty za dostawę wody i odbiór ścieków wraz z zintegrowanym z nim systemem Finansowo Księgowego (FK) oraz systemy odpowiedzialne za naliczanie podatków i pozostałych opłat realizowanych w urzedzie. Wymiana danych musi przebiegać poprzez bezpieczne, szyfrowane połączenie za pośrednictwem serwisów komunikacyjnych zainstalowanych na infrastrukturze Zamawiającego. W ramach wdrożenia systemu wymagana jest analiza bazy danych modułów systemów dziedzinowych celem określenia możliwości świadczenia oferowanych usług oraz wykonanie i dostawa takiego serwisu (wymagania określone w pkt. *WYMAGANIA DOTYCZĄCE BUDOWY MODUŁU INTEGRUJĄCEGO, SZYNA DANYCH, BROKER KOMUNIKACYJNY*)
20. Dostęp do danych indywidualnego konta klienta musi być zapewniony poprzez bezpieczne logowanie i tylko dla kont które przeszły procedurę autoryzacji.
21. Wymiana danych musi być zabezpieczona za pomocą transmisji z wykorzystaniem tokenu. Przy nieprawidłowych danych metoda nie powinna się wykonać i musi zostać zwrócony stosowny komunikat z błędem.
22. Implementacja mechanizmów polegających na automatyzacji wymiany danych pomiędzy platformą eBOM a systemem dziedzinowym (dostępność do aktualnych danych) nie może dodatkowo angażować operatorów systemów po stronie Zamawiającego.
23. Udostępnianie danych użytkownika musi następować wyłącznie po zalogowaniu się użytkownika na jego indywidualne konto.
24. Dane do wizualizacji muszą być pobierane automatycznie z bazy systemu dziedzinowego za pośrednictwem usług serwisu SOAP uruchomionego na infrastrukturze Zamawiającego. Dostęp do serwisu jest szyfrowany i zabezpieczony certyfikatem. Dane udostępniane są tylko w odniesieniu do konta danego użytkownika i po jego wiarygodnym uwierzytelnieniu.
25. Portal eBOM zalogowanemu i uwierzytelnionemu użytkownikowi musi zapewniać wizualizację danych pochodzących z systemów dziedzinowych za pomocą tabel i pól informacyjnych pogrupowanych ze względu na poszczególne obszary i kartoteki minimum w zakresie:
    1) Naliczonych opłat i wystawionych faktur,
    2) Aktualnych rozliczeń, sald kont a w przypadku zaległości wysokości należnych odsetek oraz kosztów egzekucji wg. stanu na dzień zalogowania,
    3) Informacji o podstawach naliczonych podatków i opłat (grunty, nieruchomości, działki, pozycje rejestrowe, numery ewidencyjne kartotek, indywidualne numery rachunków dla dokonywania wpłat, daty powstania należności (decyzja podatkowa, wystawiona opłata, deklaracja o wysokości opłaty za odbiór odpadów komunalnych itp.,
    4) Portal powinien udostępniać dokumenty źródłowe tworzone w systemach dziedzinowych (decyzje podatkowe, faktury, informacje podatkowe, deklaracje, zaświadczenia oraz inne dokumenty zapisywane w systemie dziedzinowym na indywidualnych kartotekach petentów) w formacie dokumentu PDF,
    5) Ewidencji układów pomiarowych wraz z danymi odczytów oraz źródłem ich pochodzenia,
    6) Wykresy zużycia wody w podziale na poszczególne układy pomiarowe,
    7) Dane historyczne dotyczące wystawionych faktur oraz decyzji podatkowych z możliwością ich pobrania w formacie PDF minimum 5 lat wstecz.
    8) Dane adresowe posesji klienta w przypadku gromadzenia takich informacji w systemie dziedzinowym w odniesieniu do danej opłaty lub podatku;
    9) Dane związane z zawartą umową (nr. umowy, data zawarcia, skan umowy papierowej jeżeli jest zapisany w systemie dziedzinowym itp.)
    10) zezwoleń na handel wyrobami alkoholowymi dla podmiotów prawnych dane dotyczące ich punktów posiadających zezwolenie na sprzedaży wyrobów alkoholowych ze

szczegółową lokalizacją (adres i nazwa punktu sprzedaży), danymi posiadanego zezwolenia, należnymi opłatami w podziale na raty i terminy ich uiszczenia.

26. Szczegółowy zakres dotyczący zobowiązań podatkowych powinien zapewnić wizualizację danych pogrupowanych ze względu na obszary i kartoteki podatnika. Dane udostępniane powinny być tylko w odniesieniu do konta danego podatnika i po jego uwierzytelnieniu.
    Zakres danych do prezentacji dla tych modułów podatkowych systemów dziedzinowych musi obejmować:
    a. W odniesieniu do Podatku od Środków Transportowych:
        - Wykazu pojazdów zgodnie ze złożoną deklaracją
        - Sprawdzenia zobowiązań wobec Urzędu w zakresie opłat za podatek od środków transportowych
        - Integracja z systemem płatności elektronicznych
        - Podgląd dokumentów (deklaracji, decyzji, innych pism) dotyczących karty podatkowej danego podatnika z możliwość ich automatycznego pobrania (w przypadku dokumentów „tradycyjnych" ich elektroniczna kopia w formacie pdf a w przypadku dokumentu elektronicznego oryginał).
    b. W odniesieniu Podatki lokalnych (rolny, leśny, od nieruchomości):
        - Sprawdzenia stanu posiadania podatnika
        - Sprawdzenia naliczonego podatku (wymiar podatku)
        - Sprawdzenia zobowiązań wobec Urzędu w tytułu podatków (rolnego, leśnego, od nieruchomości)
        - Integracja z systemem płatności elektronicznych
        - Podgląd dokumentów (deklaracji, decyzji, wystawionych zaświadczeń, innych pism) dotyczących karty podatkowej danego podatnika z możliwość ich automatycznego pobrania (w przypadku dokumentów „tradycyjnych" ich elektroniczna kopia w formacie pdf a w przypadku dokumentu elektronicznego oryginał).
    c. W odniesieniu do Ewidencji opłat za gospodarowanie odpadami komunalnymi.
        - Sprawdzenia danych zawartych umów na wywożenie odpadów
        - Sprawdzenia wystawionych przypisów / kwot do zapłaty
        - Sprawdzenia zobowiązań wobec Urzędu z tytułu rozliczeń za odpady komunalne.
        - Moduł musi być zintegrowany z systemem płatności elektronicznych, który realizuje wpłaty bezpośrednio na rachunek urzędu
        - Podgląd dokumentów (deklaracji, decyzji, informacji o wysokości opłat, innych pism) dotyczących karty danego podatnika z możliwość ich automatycznego pobrania (w przypadku dokumentów „tradycyjnych" ich elektroniczna kopia w formacie pdf a w przypadku dokumentu elektronicznego oryginał).
27. Wizualizacja zobowiązań musi zapewnić przejrzystą prezentację należności z uwzględnieniem ich sald, terminów płatności oraz wysokości odsetek wraz z ewentualnymi kosztami upomnień.
28. System musi zapewniać wyliczanie ogólnej kwoty należności oraz wysokość zależności przeterminowanych.
29. System musi wizualizować informacje z systemów dziedzinowych o dokonanych wpłatach i dawać możliwość przeglądania zobowiązań wg. zbliżających się terminów zapłaty należności.
30. Moduł powinien mieć prezentację łączną wszystkich rodzajów zobowiązań na jednej liście z możliwością zaznaczenia wielu kwot do zapłaty. W przypadku konieczności podzielenia wpłat na poszczególne rodzaje system powinien je pogrupować w „koszyki" do zapłaty i umożliwić realizacje poszczególnych wpłat za pośrednictwem systemu płatności elektronicznych.
31. Moduł musi umożliwiać użytkownikowi dokonywanie wpłat na różne faktury (należności z tytułu podatków i opłat, należności z tytułu opłaty za gospodarowanie odpadami komunalnymi, opłaty za dostawę wody, inne faktury wystawione w systemie). Przy zaznaczeniu różnych typów zobowiązań system powinien automatycznie zgrupować należności w „koszyk wpłat" i pozwolić użytkownikowi dokonywania poszczególnych wpłat oddzielnymi poleceniami. Należności stanowiące zobowiązania jednego typu powinny być płacone w jednym przelewie. System powinien dokonywać wpłaty na indywidualne rachunki przydzielone do poszczególnych należności.

32. System musi posiadać możliwość zintegrowania z co najmniej dwoma systemami płatniczymi. Systemy płatnicze powinny posiadać zezwolenie Komisji Nadzoru Finansowego na świadczenie usług płatniczych w charakterze krajowej instytucji płatniczej lub realizować bezpośrednie płatności z konta płatnika na rachunek urzędu.
33. System musi pozwalać na wnoszenie opłat za pośrednictwem systemu płatności elektronicznych w sposób umożliwiający wygenerowanie płatności na wybraną należność i jej opłacenie, lub na zaznaczenie kilku należności tego samego typu i zapłacenie ich jednym przelewem.
34. System musi dawać możliwość sortowania wyświetlanych danych rosnąco lub malejąco względem wyświetlanych parametrów należności. Zapewnić możliwość wyszukiwania lub filtrowania należności według ich rodzajów i terminów płatności (dat).
35. System zapewni wizualizację zaksięgowanych operacji na należnościach (wpłaty, zwroty, przeksięgowania) z wyszczególnionym informacji na jaką należności została zaksięgowana oraz salda pozostałego do zapłaty.
36. System musi posiadać mechanizmy kontroli i bezpieczeństwa chroniące użytkowników przed kilkukrotnym wniesieniem płatności z tego samego tytułu. System musi generować komunikaty informujące i/lub ostrzeżenia wizualne dla użytkownika podczas próby ponownego zlecenia płatności dla należności, dla których płatność została zlecona za pośrednictwem Portalu, a transakcja jeszcze jest przetwarzana.
37. System musi dawać możliwość wydrukowania wypełnionego polecenia przelewu bankowego dla zaznaczonej należności (faktury).
38. System musi dawać możliwość wysyłania przypomnień o terminie płatności za pośrednictwem systemu komunikacji elektronicznej z interesantem, (wymagane kanały komunikacji elektronicznej: email, sms, komunikat push na aplikację mobilną). Indywidulane terminy płatności zobowiązań powinny być także wyświetlane uwierzytelnionym użytkownikom systemu w module kalendarzy (harmonogramów).
39. Wygenerowane płatności zlecone za pośrednictwem systemu, ale jeszcze nie zaksięgowane muszą zawierać informacje takie jak: nr konta bankowego na które została przelana płatność, kwota i data zlecenia, status zlecenia oraz data wykonania.
40. W zakresie integracji z systemem ePłatności (PeP) oferowanym w ramach aplikacji mObywatel platforma eBOM musi umożliwić dwukierunkową wymianę danych zgodną z wymaganiami określonymi przez jej administratora w dokumentacji technicznej interfejsu API dla Urzędów Administracji Publicznej autorstwa Centralnego Ośrodka Informatyki. Wykonawca będzie zobowiązany do zachowania zgodności z oferowanym interfejsem API oraz będzie musiał przejść testy integracyjne zgodne z wymaganiami administratora tej platformy.
41. Platforma eBOM powinna zapewnić wizualizację stanów należności przekazaną do systemu PeP na koncie podatnika przez bezpośrednie sprawdzenie statusu za pośrednictwem API systemu PeP.

Komunikaty, powiadomienia i ogłoszenia, aktualności

42. System ma zapewnić możliwość przesyłania spersonalizowanych komunikatów do petentów generowanych na podstawie zdarzeń występujących w systemie dziedzinowym oraz komunikatów wprowadzonych „ręcznie” przez administratora systemu.
43. System powinien posiadać jedną kartotekę komunikatów zawierającą informację o treści komunikatu, źródło jego pochodzenia, dacie zapisania do rejestru, identyfikację odbiorcy, datę i godzinę wysłania, datę ważności komunikatu oraz identyfikację kanału którym został on przesłany.
44. Administrowanie i zarządzanie kontami użytkowników odbywać się będzie z poziomu panelu administratora portalu eBOM.
45. Administrator powinien mieć dostępny edytor wzorów treści dla określonych typów komunikatów oraz wybranego kanału dystrybucji.
46. W systemie powinny być dostępne kanały komunikacyjne za pośrednictwem SMS-a, e-maila oraz komunikatu push do aplikacji mobilnych.
47. Wysyłanie komunikatów powinno być wykonywane wg. kryteriów (kalendarzy) określonych przez administratora.

48. System powinien współpracować z modułami dziedzinowymi w zakresie powiadamia co najmniej o:
    - Zbliżający się termin płatności zobowiązania
    - Przypomnienie o zaległościach
    - Wystawienie nowego dokumentu dla użytkownika na portalu (faktura, decyzja podatkowa, deklaracja, umowa, informacja itp.)
    - Dokonanie księgowania na koncie podatnika (zaksięgowanie wpłaty, przeksięgowanie nadpłaty, dokonanie korekty należności, wystawienie upomnienia)
40. System w zakresie ogłoszeń musi umożliwić operatorowi prowadzenie serwisu aktualności z uwzględnieniem możliwości wprowadzania minimum:
    A) Opisu wydarzenia (zdarzenia)
    B) Terminu
    C) Wprowadzenia adresu www do pełnej informacji o danym zdarzeniu
    D) Wprowadzenie lokalizacji z wizualizacja na mapie
    E) Wprowadzenie zdjęcia głównego do wyświetlania na liście aktualności
    F) Wprowadzenie ewentualnych dodatkowych zdjęć wraz z opisami
41. Aktualności (ogłoszenia) powinny być dostępne zarówno dla użytkownika zalogowanego jak i niezalogowanego.
42. Administrator portalu powinien mieć możliwość włączenia lub wyłączenia wizualizacji tego modułu dla użytkowników. Opcja ta powinna dotyczyć zarówno portalu jak i aplikacji mobilnej.
43. Oprócz aktualności wprowadzanych „ręcznie" przez operatora systemu powinna być możliwość publikowania w aktualnościach kanału RSS pobieranego z innego serwisu.
44. Aktualności powinny się wyświetlać w liście w układzie chronologicznym z uwzględnieniem na liście krótkiego opisu, nazwy oraz zdjęcia tytułowego.
45. Wspólna lista aktualności powinna zawierać zarówno wiadomości wprowadzone przez operatora jak i te pobrane z kanału RSS ułożone w porządku chronologicznym.
46. Użytkownik systemu powinien mieć możliwość subskrybowania powiadomień dotyczących aktualności.

Kalendarze (harmonogramy odczytów, wywozów odpadów, ustawowych terminów płatności podatków itp.)

47. Moduł powinien wyświetlać kalendarz wraz z naniesionymi wpisami dokonanymi przez administratora systemu.
48. Kalendarz powinien być wyświetlany w układzie miesięcznym oraz listy.
49. Wpisy w kalendarzu powinny być typizowane z możliwością przydzielenia im znaków graficznych oraz nadania koloru wyświetlania.
50. Użytkownik powinien mieć możliwość subskrybowania powiadomień dla wybranego typu harmonogramu.
51. Powinna być możliwość wprowadzenia zdarzeń do kalendarza pojedynczych na wybrany dzień jak i okresowych z uwzględnieniem terminu powtarzania minimum w zakresie wybranego dnia tygodnia, zdarzeń powtarzalnych w dany dzień w miesiącu, zdarzeń cyklicznych (np. ostatni dzień miesiąca, co dwa tygodnie itp.)
52. Wymagane jest określenie końcowej daty występowania danego zdarzenia cyklicznego w harmonogramie.
53. Użytkownik powinien mieć możliwość wybrania na kalendarzu zakresu wyświetlania zdarzeń (harmonogramów). W przypadku użytkownika zalogowanego powinna być możliwość zapisania wybranych ustawień na jego koncie.
54. W przypadku użytkownika zalogowanego na kalendarzu powinny się wyświetlać terminy płatności zobowiązań pobrane z sytemu bilingowego wraz z podaniem kwoty należności, tytułu zapłaty oraz numeru rachunku bankowego na który należy dokonać płatności.
55. Harmonogramy powinny mieć określone typy, kolory do prezentacji na widoku kalendarza oraz znaki graficzne. W obrębie typów powinien być minimum jeszcze jeden słownik dla wyróżnienia w jego obrębie podtypu (np. harmonogram wywozu odpadów podzielony na miejscowości a w ich obrębie rodzaje wywożonych frakcji odpadów). Wprowadzony podział powinien mieć odzwierciedlenie w ustawieniach filtrowania harmonogramów przez użytkownika systemu.

56. W szczególności system powinien umożliwić obsługę harmonogramów wywozów odpadów. Użytkownik powinien mieć możliwość prezentacji tych terminów zarówno w układzie kalendarza jak i listy. Dla zalogowanych użytkowników powinna być możliwość określenia które harmonogramy mają być dla niego wyświetlane w kalendarzu. Harmonogramy powinny umożliwić podział na trasy wywozu oraz rodzaje odpadów.

Informacji podstawowe (dane adresowe, numery kont, godziny urzędowania itp.)

57. System powinien umożliwić wyświetlenie danych podstawowych Zamawiającego
58. Panel CMS administratora powinien operatorowi umożliwić wprowadzenie samodzielne tych danych.
59. System powinien zapewnić czytelną wizualizację wprowadzonych danych z uwzględnieniem zamieszczonych znaków graficznych (logotypy itp.)
60. W miarę możliwości wizualizacja tych danych powinna być spójna na platformie eBOM i po stronie aplikacji mobilnej

Karty usług (eUsługi)

61. System powinien umożliwić publikowanie kart usług w ustandaryzowany sposób.
62. W zakresie wprowadzania kart usług powinna być możliwość zdefiniowania przez operatora haseł tematycznych koniecznych do wypełnienia przy wprowadzaniu opisu danej e-Usługi.
63. Karty usług powinny mieć możliwość powiązania ze słowami kluczowymi a użytkownik powinien mieć możliwość wyszukiwania kart na ich podstawie.
64. Panel CMS powinien być wyposażony w edytor treści umożliwiający wprowadzenie opisów usług z uwzględnieniem podstawowych funkcji takich jak formatowanie tekstu, rodzaj czcionki, odnośniki do stron www, znaki wypunktowania, justowania itp.
65. Powinna być możliwość przydzielania kart usług do skorowidzu tematycznego zdefiniowanego przez operatora. Przeglądanie list spraw powinno uwzględniać ten przydział. W zakresie przeszukiwania treści publikowanych kart e-Usług portal eBOM musi pozwalać na wyszukiwanie po opisie i nazwie usługi oraz słowach kluczowych przyporządkowanych do danej usługi.
66. Wyszukiwanie powinno też obejmować opis usługi który powinien być oddzielnym polem do wprowadzenia i być wyświetlany na liście usług.
67. System powinien umożliwić dodawanie do kart usług załączników (wzorów formularzy) w formie edycyjnej oraz do wydruku (PDF).
68. Operator powinien mieć możliwość dodania do karty usługi dokumentów (klauzul) wymaganych do pobrania przez użytkownika przed przejściem realizacji danej usługi.
69. Operator powinien mieć możliwość dodania do karty usługi płatności elektronicznej z określeniem numeru rachunku, danych wierzyciela, tytułu wpłaty, kwoty. Wymagana jest możliwość określenia czy użytkownik końcowy na etapie realizacji płatności będzie mógł edytować tytuł wpłaty i kwotę. Płatność powinna być realizowana elektronicznie przez wybrany i skonfigurowany system płatności elektronicznych.
70. Operator powinien mieć możliwość powiązania danej usługi z procedurą elektroniczną na platformie ePUAP, lub innym serwisie usługowym wykorzystywanym w urzędzie. Procedura wywołanie tych eUsług powinna być widoczne z poziomu danej karty i ułatwić maksymalnie użytkownikowi przekierowania na konkretną stronę i realizowaną na niej procedurę.
71. W zakresie e-Usług związanych z wydawaniem pozwoleń na sprzedaż wyrobów alkoholowych portal eBOM powinien mieć wbudowany kalkulator naliczania opłaty z uwzględnieniem rodzaju pozwolenia, wielkości sprzedaży oraz dat obowiązywania zezwolenia.
72. W zakresie kart usług portal eBOM musi umożliwiać Klientowi na złożenie wniosku i zainicjowanie sprawy. Usługa powinna być realizowana przez platformę ePUAP gdzie Klient powinien mieć możliwość podpisywania wniosków/formularzy zaufanym profilem ePUAP. eBOM musi integrować się z platformą ePUAP (logowanie ePUAP, logowanie profilem zaufanym). Musi umożliwiać wskazanie formularza umieszczonego na ePUAP w karcie usługi na portalu.
73. *W ramach uruchomienia i konfiguracji platformy eBOM* Wykonawca przygotuje i zainstaluje na niej przykładowe e-Usługi wraz z opracowaniem kartami usługi oraz niezbędnymi formularzami

na platformie ePUAP. Wykonawca zapewni aktualność uruchomionych formularzy elektronicznych przez okres trwania gwarancji i asysty technicznej. Lista e-Usług realizowanych w ramach zamówienia (dla każdej e-Usługi musi zostać przygotowany na platformie ePUAP odpowiadający jej formularz, umożliwiający realizację e-Usługi na wskazanym poziomie dojrzałości). Zakres usług zostanie określony na etapie realizacji.

Wymogi w zakresie tworzenia formularzy ePUAP:

a) Formularze stosowane na ePUAP powinny być tworzone z wykorzystaniem języka XForms oraz XPath.
b) Wykonawca opracuje formularze elektroniczne (zgodnie z właściwymi przepisami prawa) na podstawie przekazanych przez Zamawiającego kart usług z formularzami w formacie edytowalnym lub wykorzysta w celu realizacji e-Usługi formularze usług centralnych.
c) Wszystkie formularze elektroniczne Wykonawca przygotuje z należytą starannością tak, aby pola do uzupełnienia w tych formularzach zgadzały się z polami formularzy w formacie edytowalnym.
d) Pola wskazane przez Zamawiającego jako pola obowiązkowe w formularzach w formacie edytowalnym, musza zostać polami obowiązkowymi również w formularzach elektronicznych.
e) Układ graficzny wszystkich formularzy powinien być w miarę możliwości jednolity. Wizualizacja formularzy elektronicznych nie musi być identyczna ze wzorem w formacie edytowalnym, ale musi zawierać dane w układzie niepozostawiającym wątpliwości co do treści i kontekstu zapisanych informacji, w sposób zgodny ze wzorem.
f) W miarę możliwości przygotowując formularze Wykonawca musi dążyć do maksymalnego wykorzystania słowników.
g) W budowanych formularzach należy wykorzystać mechanizm automatycznego pobierania danych z profilu zaufanego – celem uzupełnienia danych o wnioskodawcy.
h) Formularze muszą zapewniać walidację wprowadzonych danych po stronie klienta i serwer zgodnie z walidacją zawartą w schemacie dokumentu.
i) Każdy opracowany przez Wykonawcę formularz (w postaci pliku XML) musi zostać przekazany Zamawiającemu w celu dokonania sprawdzenia i wykonania testów na formularzu. Po okresie testów Zamawiający przekaże Wykonawcy ewentualne poprawki i uwagi dotyczące poszczególnych formularzy, które Wykonawca usunie w ciągu 7 dni.
j) Wykonawca przygotuje wzory dokumentów elektronicznych zgodnie ze standardem ePUAP w formacie XML zgodnym z formatem Centralnego Repozytorium Wzorów Dokumentów. Wykonawca ma obowiązek sprawdzenia poprawności przygotowanych formularzy. Zamawiający dopuszcza możliwość wykorzystania przez Wykonawcę wzorów, które są już opublikowane w CRWD po akceptacji Zamawiającego.
k) Wygenerowane dla poszczególnych formularzy wzory dokumentów elektronicznych, składając się z: Wyróżnika (wyroznik.xml); Schematu (schemat.xml); Wizualizacji (styl.xsl) muszą zostać dostosowane do wymogów formatu dokumentów publikowanych w CRWD.
l) W ramach wdrożenia Wykonawca przygotuje i przekaże Zamawiającemu wszystkie wzory dokumentów elektronicznych w celu złożenia wniosków o ich publikację w CRWD. Wykonawca udzieli wsparcia Zamawiającemu w przejściu procesu publikacji na ePUAP. Bazując na przygotowanych wzorach dokumentów elektronicznych oraz opracowanych na platformie ePUAP formularzach elektronicznych Wykonawca przygotuje instalacje aplikacji w środowisku ePUAP.

74. Zaimplementowane formularze muszą spełniać wymogi ePUAP oraz pozytywnie przechodzić przeprowadzone na ePUAP walidacje zgodności ze wzorami dokumentów. Na czas realizacji projektu Zamawiający zapewni Wykonawcy dostęp do części administracyjnej platformy ePUAP konta JST z uprawnieniami do konsoli administracyjnej Draco, ŚBA i usług. W przypadku zwłoki w publikacji wzorów dokumentów CRWD realizowanej przez Ministerstwo Cyfryzacji (administrator ePUAP) dopuszcza się dokonanie odbioru tej części zamówienia w ramach lokalnej publikacji w CRWD z zastrzeżeniem, że Wykonawca dokona przekonfigurowania aplikacji po pomyślnej publikacji CRWD przez Ministerstwo Cyfryzacji.
75. Zamawiający przekaże Wykonawcy opisy usług w formacie edytowalnym.

76. Zamawiający dopuszcza, aby Wykonawca wykorzystał opisy usług, które są umieszczone na platformie ePUAP po akceptacji opisu usługi przez Zamawiającego. Zadaniem Wykonawcy jest odpowiednie powiązanie opisów usług zamieszczonych na ePUAP z odpowiednimi usługami na platformie eBOM.

Zarządzane portalem eBOM - panel Administratora CMS

77. Administracja systemem powinna być wspólna z danymi prezentowanymi w aplikacji mobilnej.
78. Logowanie do panelu administratora powinno być zabezpieczone loginem i hasłem oraz możliwością ograniczenia dostępu dla wybranych adresów IP.
79. System zapewnia podgląd listy użytkowników, którym udostępniono dostęp do Portalu, wraz z danymi dotyczącymi, nazwy, identyfikatora, adresu e-mai, daty utworzenia konta, statusu oraz metody logowania.
80. Administrator ma podgląd do informacji o próbach logowania do systemu ze wskazaniem identyfikatora, daty, adresu IP z którego nastąpiło połączenie do portalu.
81. System powinien uwzględniać możliwość definiowania wielu kont administracyjnych i określenia zakresu danych dostępnych do wprowadzania dla danego konta.
82. Konto administratora głównego urzędu powinno mieć możliwość dodawania przez niego administratorów lokalnych z określonym przez niego poziomem dostęp do edycji treści publikowanych w portalu.
83. Panel CMS musi zapewnić wprowadzenie danych celem osiągnięcia funkcjonalności opisanych powyżej.
84. Panel CMS powinien mieć przejrzystą formę wprowadzania informacji opartą o formularze i wspólne słowniki dla danych powtarzających się.
85. Pola do edycji danych tekstowych wymagających wprowadzenia formatowania dla potrzeb wizualizacji w portalu eBOM powinny mieć edytor treści zapewniający sprawne formatowanie wprowadzanego tekstu.
86. Panel zarządzania treścią powinien być wspólny dla portalu eBOM oraz aplikacji mobilnej.
87. Z poziomu panelu CMS administratora powinny być realizowane wymagania dotyczące wysyłki powiadomień.
88. Konfiguracja połączeń z systemami zewnętrznymi (system dziedzinowy urzędu, Krajowy Węzeł Identyfikacji Elektronicznej, bramka SMS, klient pocztowy e-MAIL, wybrany system płatniczy, platforma ePłatności [PeP]) powinna być możliwa z poziomu konta administratora głównego. Administrator powinien po stronie panelu CMS mieć możliwość wgrania odpowiednich certyfikatów oraz ustawienia wymaganych haseł oraz innych parametrów charakterystycznych dla tych systemów
89. Panel CMS powinien mieć tryb automatycznej wizualizacji treści wprowadzonych zmiana z poziomu konta administratora w układzie docelowym zgodnym z widocznością użytkownika docelowego portalu eBOM zarówno w zakresie treści dostępnych dla użytkowników niezalogowanych jak i zalogowanych i uwierzytelnionych (podgląd kartoteki bilingowej).
90. Panel administratora powinien umożliwić przeglądanie logów z operacji wymiany danych z platformą ePłatności (PeP).
91. Administrator powinien mieć możliwość ustawienia terminów (godzin) operacji wysyłania i pobierania danych z platformy ePłatności (PeP).

7.3. Planowanie budżetu – licencja szt. 1 – wymagania minimalne

Wymagania funkcjonalne modułu planowania budżetu.

Moduł musi spełniać następujące wymagania funkcjonalne :

1. System powinien być dostępny we wszystkich wydziałach urzędu oraz dla wszystkich jednostek organizacyjnych.
2. System powinien służyć do wspomagania obsługi procedur budżetowych w zakresie planowania, zarządzania, zaangażowania i realizacji.
3. Moduł do planowania budżetu powinien być dostępny niezależnie od posiadanych systemów finansowo-księgowych w poszczególnych jednostkach, jednocześnie powinien być połączony z systemem finansowo - księgowym jednostki nadrzędnej.
4. Moduł powinien być powiązany z innymi modułami systemu dziedzinowego poprzez:
    - pracę na wspólnej bazie danych;

- wykorzystywanie wspólnych słowników systemowych co najmniej w zakresie kartoteki kontrahentów, prowadzonych inwestycji, zadań Funduszu Sołeckiego, zadań Funduszu Osiedlowego;
- słowników klasyfikacji oraz zadań budżetowych;

5. Moduł do planowania budżetu powinien być dostępny poprzez przeglądarkę internetową.
6. Moduł powinien posiadać dwa obszary pracy:
   - Strefa użytkownika zalogowanego – prowadzenie prac związanych z projektowaniem budżetu oraz nadzorem nad jego realizacją;
   - Strefa otwarta – udostępnienie informacji o realizowanym budżecie, prowadzonych inwestycjach, udzielonych dotacjach itp. jako forma prezentacji bez możliwości modyfikacji.
7. Moduł powinien składać się z obszarów funkcjonalnych (podmodułów) odpowiadających za:
   - projektowanie plany oraz obsługę zmian w budżecie JST;
   - nadzór na zaangażowaniem planu;
   - nadzór nad stanem realizacji wydatków budżetowych;
   - sprawozdawczości budżetowej

Planowanie budżetu:

1. Moduł do planowania budżetu powinien umożliwiać tworzenia struktury organizacyjnej jednostki z podziałem na obszary planistyczne składające się z jednostek organizacyjnych, wydziałów, placówek, samodzielnych dysponentów środków.
2. Moduł powinien umożliwiać tworzenia planów jednostkowych na poziomie jednostek, wydziałów, placówek oraz samodzielnych dysponentów środków.
3. Moduł powinien posiadać możliwość nadawania uprawnień dla poszczególnych użytkowników w zakresie dostępu do poszczególnych jednostek jak i funkcjonalności systemu.
4. Moduł do planowania budżetu powinien umożliwiać projektowanie budżetu w układzie:
   - ***Grup klasyfikacji budżetowej*** *- Dział/Rozdział/Grupa wydatków/Pochodzenie*
   - ***Klasyfikacji budżetowej z analityką*** *- Dział/Rozdział/Paragraf/Analityka budżetowa (tytuły wydatków i dochodów)*
   - ***Zadań budżetowych*** *Wydział/Zadanie/Rodzaj(bezpośrednie, pośrednie, inwestycyjne, dochodowe/Kategoria (własne, zlecone, powierzone, porozumienie, porozumienie JST*).
5. Moduł do planowania budżetu powinien posiadać możliwość definiowania struktury analityki budżetowej składającej się z elementów słownikowych identyfikującej co najmniej takie obszary jak:
   - dysponent środków,
   - realizowane zadnie (oddzielnie dla wydatków i dochodów),
   - realizowany projekt ze środków zewnętrznych,
   - źródło finansowania,
   - pochodzenia.
6. Moduł powinien umożliwić definiowania obszarów pracy dla poszczególnych jednostek planistycznych tzn. ograniczenie wartości słownikowych w obrębie których jednostka będzie mogła dokonywać wyboru przy tworzeniu dokumentu planistycznego. Dotyczy to słowników: rozdziałów budżetowych, źródeł finansowania oraz zadań.
7. Moduł powinien umożliwiać prowadzenie Funduszu Sołeckiego w rozbiciu na poszczególne miejscowości i przedsięwzięcia wchodzące w jego skład.
8. Moduł powinien posiadać możliwość powiązania zadań lub innych elementów słownikowych z wybraną miejscowością Funduszu Sołeckiego.
9. Moduł powinien umożliwiać prowadzenie Funduszu Osiedlowego w rozbiciu na poszczególne osiedla, dzielnice i przedsięwzięcia wchodzące w jego skład.
10. Moduł powinien posiadać możliwość powiązania zadań lub innych elementów słownikowych z wybranym osiedlem, dzielnicą Funduszu Osiedlowego.
11. Moduł powinien posiadać możliwość tworzenia słownika inwestycji zawierającego co najmniej takie informacje jak:
    - numer, symbol inwestycji;

- opis inwestycji;
- rok rozpoczęcia;
- rok zakończenia;
- kategoria;
- cel;
- limit wydatków.

12. Moduł powinien posiadać możliwość tworzenia słownika udzielonych dotacji oraz ich beneficjentów.
13. Moduł powinien umożliwiać parametryzację udzielonej dotacji z uwzględnieniem takich parametrów jak:
    - rodzaj dotacji: podmiotowa, celowa, przedmiotowa;
    - cel dotacji – przeznaczenie;
    - beneficjent dotacji – podmiot;
    - typ dotacji wynikający z typu podmiotu (publiczny lub nie).
14. W systemie powinno być możliwe wprowadzenie limitów środków rzeczowych, limitów na etaty, wyliczenie kosztu roboczogodziny w danej komórce, tworzenie bieżących wydatków, tworzenie wersji zadań bezpośrednich, tworzenie zadań inwestycyjnych, tworzenie zadań dochodowych, tworzenie zadań wydziałowych, wprowadzenie planu przychodów i wydatków funduszy celowych, rezerw itp.
15. Moduł powinien umożliwiać procedowania tworzenia budżetu jednostki w podziale na etapy: projekt budżetu, korekta projektu budżetu, projekt budżetu po korekcie, plan budżetu uchwalony , zmiany do planu budżetu. Na każdym etapie pracy system powinien umożliwiać weryfikację danych przez służby Skarbnika.
16. Moduł powinien umożliwiać dokonywania operacji w obrębie dokumentów planistycznych takich jak:
    - przesłanie do jednostki nadrzędnej;
    - zatwierdzenie przez jednostkę nadrzędną;
    - zwrot do jednostki podległej;
    - autokorekta służb Skarbnika (poprawa planów jednostkowych bez konieczności zwrotu do jednostki podległej);
17. Moduł powinien umożliwiać tworzenie załączników do dokumentów planistycznych zawierających szczegółowe informacje dotyczące:
    - Załącznik klasyfikacyjny (wydatki, dochody, przychody, rozchody) zawierający takie informacje jak: Plan przed zmianą, Zwiększenie, Zmniejszenie, Plan po zmianie;
    - Załącznik: Kadry i płace – tabela kalkulacyjna;
    - Załącznik inwestycyjny zawierający informacje dotyczące przedsięwzięć z uwzględnieniem ich podziału na klasyfikację budżetową ;
    - Załącznik inwestycyjny zawierający informację o klasyfikacjach budżetowych w których są realizowane poszczególne inwestycje;
    - Załącznik: Inwestycyjny – tabela kalkulacyjna;
    - Załącznik informacja o udzielonych dotacjach z uwzględnieniem ich podziału na klasyfikacje budżetową;
    - Załącznik informacja o udzielonych dotacjach o klasyfikacjach budżetowych uwzględnieniem ich podziału beneficjentów i cele dotacyjne;
    - Załącznik zestawienie wydatków i dochodów w podziale na grupy klasyfikacyjne z uwzględnieniem pochodzenia środków;
    - Załącznik wydatków na przedsięwzięcia ujęte w WPF;
    - Załącznik wydatków na programy finansowane z udziałem środków z budżetu UE;
    - Załącznik wykaz zobowiązań z tytułu zawartych umów – tabela kalkulacyjna;
    - Załącznik dochody z tytułu gospodarki nieruchomościami – tabela kalkulacyjna;
    - Załącznik Fundusz Sołecki zawierający informacje dotyczące przedsięwzięć z uwzględnieniem ich podziału na klasyfikację budżetową;
    - Załącznik Fundusz Sołecki zawierający informacje o klasyfikacjach budżetowych w których są realizowane poszczególne przedsięwzięcia;

- Załącznik Fundusz Osiedlowy zawierający informacje dotyczące przedsięwzięć z uwzględnieniem ich podziału na klasyfikację budżetową;
- Załącznik Fundusz Osiedlowy zawierający informacje o klasyfikacjach budżetowych w których są realizowane poszczególne przedsięwzięcia.

18. Załączniki do dokumentów planistycznych w poniższych obszarach powinny mieć strukturę tabel kalkulacyjnych umożliwiających wprowadzanie danych w zakresie:
    - ***Kadry i płace***: stanowisko, etat, wynagrodzenie brutto, rodzaj podwyżki (% lub kwota), podwyżka, dodatek funkcyjny, % dodatku stażowego, dodatek stażowy, dodatek specjalny, % premii, kwota premii, inne, razem wynagrodzenie miesięczne, razem wynagrodzenie roczne, % funduszu nagród, fundusz nagród, nagroda jubileuszowa, odprawa, ekwiwalent, rozdział klasyfikacji budżetowej; opis do pozycji;
    - ***Inwestycje:*** Nazwa inwestycji, Klasyfikacja budżetowa (dział, rozdział, paragraf), planowana wartość wg kosztorysu, wartość wydatków w roku bazowym, wartość wydatków w roku poprzednim, wartość wydatków w kolejnych trzech latach, specyfikacja finansowania inwestycji (środki własne, dotacje , kredyty, pozostałe), opis inwestycji, okres realizacji;
    - ***Umowy:*** Nazwa umowy, klasyfikacja budżetowa, Nazwa podmiotu, NIP, całkowita kwota umowy, kwota realizowana w roku bazowym, szczegółowy opis umowy, okres obowiązywania
    - ***Gospodarka nieruchomościami:*** Nazwa; opis nieruchomości, numer działki, powierzchnia działki, przewidywana kwota dochodów.
19. Wszystkie dokumenty generowane przez system muszą być eksportowane do innych plików pdf, docx, excel, rtf, odt, ods, html, csv z możliwością ich edycji.
20. Moduł powinien mieć możliwość ustawienia statusu dostępu w zależności od nadania uprawnień.
21. Moduł powinien umożliwiać opracowanie projektu budżetu i możliwości eksportu do systemu bestia. Powinien również zawierać możliwość przygotowania projektu uchwały budżetowej, jak również różnych innych wydruków (załączników do budżetu) według wzorów wprowadzonych przez jednostkę.
22. Przygotowanie budżetu powinno opierać się o słowniki wydatków podpięte pod odpowiednie paragrafy klasyfikacji budżetowej. W przypadku zmiany rozporządzenia dotyczącego klasyfikacji budżetowej system powinien automatycznie uaktualniać słowniki.
23. Moduł powinien umożliwiać opracowanie projektu budżetu i możliwości eksportu budżetu i wszystkich załączników do systemu BeSti@. Powinien również zawierać możliwość przygotowania projektu uchwały budżetowej, jak również różnych innych wydruków (załączników do budżetu) według wzorów wprowadzonych przez jednostkę.
24. Moduł powinien współpracować z innymi systemami w zakresie przesyłania danych, jeżeli będzie możliwość to przesyłanie danych z innych systemów powinno być zautomatyzowane, w innym przypadku za pomocą pliku xml.
25. W zakresie integracji z systemem finansowo - księgowym proces przekazywania zmian dotyczących zatwierdzonych uchwał i zarządzeń powinien być zrealizowany w sposób automatyczny tzn. przesłanie paczki danych bezpośrednio pomiędzy strukturami bazy systemu dziedzinowego.
26. Przygotowanie budżetu powinno opierać się o słowniki wydatków podpięte pod odpowiednie paragrafy klasyfikacji budżetowej. W przypadku zmiany rozporządzenia dotyczącego klasyfikacji budżetowej system powinien automatycznie uaktualniać słowniki.
27. Moduł powinien umożliwiać wprowadzanie zmian w budżecie z opcją włączenia jednostek organizacyjnych oraz pracowników merytorycznych w proces wnioskowania o zmianę istotnych parametrów zadania. Wnioski powinny być składane w module i automatycznie zaczytywane do projektu budżetu.
28. Prezentacja danych powinna być możliwa w dowolnym układzie, np. układ budżetu, układ wykonawczy, układ Zwiększenia – Zmniejszenia, budżet Organu w układzie z jednostkami, z rodzajami zadań: własne zlecone, porozumienia, w podziale na grupy paragrafów np. dochody bieżące i majątkowe, układ wg źródeł dochodów oraz źródeł finansowania po wydatkach, przesunięcia na zadaniach inwestycyjnych, zmiany nakładów i finansowania na WPF.
29. Moduł powinien ewidencjonować wszystkie dokumenty wpływające na zmiany w budżecie.

30. Moduł, po każdej zmianie w budżecie, powinien utworzyć układ wykonawczy dla każdej z jednostek (wydziału) oraz plik w formie elektronicznej w celu rozdysponowania ich do jednostek organizacyjnych.
31. Moduł powinien mieć rozbudowany i elastyczny system słowników, możliwość dowolnego grupowania zadań i paragrafów oraz definiowanie wyglądu wydruku za pomocą zewnętrznych formatek, umożliwiać samodzielne określanie zawartości i postaci wydruków, załączników do uchwał i zarządzeń.
32. Moduł powinien umożliwiać wyodrębnienie powiatowej/gminnej części budżetu oraz każdej jednostki budżetowej.

Projektowanie i nadzór nad zaangażowaniem planu:

1. Moduł powinien być dostępny dla wszystkich pracowników wydziałów merytorycznych jednostki nadrzędnej.
2. Powinien umożliwiać wprowadzanie, kontrolę i weryfikację wszystkich dokumentów wpływających na zaangażowanie planu.
3. Moduł powinien umożliwiać wprowadzania projektów umów oraz wniosków zakupowych związanych z realizacją wydatków budżetowych.
4. Moduł powinien umożliwiać wprowadzanie charakterystycznych cech procedowanych dokumentów.
5. W zakresie wniosków zakupowych moduł powinien umożliwiać wprowadzenie informacji co najmniej takich jak:
    - Wybór wskazanie procedury zakupowej (zdefiniowane zgodnie z regulaminem ustalonym w jednostce);
    - Datę wniosku;
    - Opis przedsięwzięcia;
    - Numer sprawy;
    - Wskazanie komórki organizacyjnej kierującej wniosek;
    - Nazwę i adres wykonawcy lub wykonawców zamówienia;
    - Opis szczegółowy;
    - Rodzaj zamówienia: usługa, roboty budowlane, dostawa, inne;
    - Wartość zamówienia wyrażoną w kwocie netto i brutto;
    - Termin realizacji wniosku;
    - Numer z planu zamówień;
    - Skład Komisji przetargowej z podaniem nazwiska i imienia oraz roli rozwijane w formie tabeli danych;
    - Propozycję kryteriów oceny rozwijane w formie tabeli danych;
    - Informacje wydziału weryfikującego o zabezpieczeniu środków w budżecie jednostki;
    - Informacje wydziału weryfikującego o zgodność z planem zamówień publicznych.
6. W zakresie projektów umów moduł powinien umożliwiać wprowadzenie informacji co najmniej takich jak:
    - Rodzaj umowy;
    - Typ umowy;
    - Tryb w jakim umowa była procedowana (regulamin jednostki związany z planem zamówień publicznych)
    - Czas realizacji – okres od do;
    - Datę zawarcia;
    - Opis szczegółowy umowy
    - Numer zewnętrzny;
    - Numer wewnętrzny;
    - Kwotę brutto umowy;
    - Informację o statusie realizacji: zakończona, w trakcie realizacji itp.
    - Informacje o statusie publikacji: niepublikowana, publikowana, publikowana z opisem, publikowana z kontrahentem;
7. Moduł powinien umożliwiać podgląd bieżącego stanu realizacji budżetu z uwzględnieniem uprawnień np. widok tylko klasyfikacji związanych z wydziałem zalogowanego operatora.

8. Moduł powinien prezentować dane budżetowe (na wybrany dzień) bezpośrednio z systemu finansowo – księgowego w następującym zakresie:
    - Plan bieżący;
    - Zaangażowanie środków RB – wynikające z zaksięgowanych dokumentów;
    - Różnica pomiędzy planem a wartością zaangażowania RB;
    - % Zaangażowania środków w planie budżetowym;
    - Wydatki budżetowe – wynikające z zaksięgowanych dokumentów;
    - Różnica pomiędzy planem a wartością zrealizowanych wydatków;
    - % Realizacji wydatków w planie budżetowym
9. Moduł powinien umożliwiać przypisanie klasyfikacji budżetowych wraz z cząstkowymi kwotami stanowiącymi sumarycznie wartość kwoty planowanych wydatków
10. Moduł powinien umożliwiać dokonywanie weryfikacji kwotowych projektów dokumentów celem sprawdzenia zasadności ich przeprowadzenia.
11. Moduł powinien umożliwiać zapis statusu i kwot przeprowadzonych weryfikacji.
12. Moduł powinien umożliwić wielostopniowe dokonywanie procedury weryfikacji zarówno pod względem formalnym jak i kwotowym z uwzględnieniem następujących etapów:
    - dla dokumentów wniosków zakupowych:
        - ✓ Weryfikacja finansowo - merytoryczna na poziomie pracownika wydziału zamawiającego;
        - ✓ Weryfikacja finansowo - merytoryczna na poziomie dyrektora wydziału zamawiającego;
        - ✓ Weryfikacja finansowa na poziomie Wydziału Finansów i Budżetu – zabezpieczenie środków w budżecie;
        - ✓ Weryfikacja finansowo – merytoryczna na poziomie pracownika Wydziału Zamówień Publicznych;
        - ✓ Weryfikacja finansowo – merytoryczna na poziomie dyrektora Wydziału Zamówień Publicznych
        - ✓ Weryfikacja – zatwierdzenie przez Skarbnika;
    - dla dokumentów umów:
        - ✓ Weryfikacja finansowo - merytoryczna na poziomie pracownika wydziału sporządzającego umowę;
        - ✓ Weryfikacja finansowa na poziomie Wydziału Finansów i Budżetu – zabezpieczenie środków w budżecie;
        - ✓ Weryfikacja – zatwierdzenie przez Skarbnika - Kontrasygnata;
13. Moduł powinien umożliwiać przypisanie do dokumentu wniosku zakupowego dodatkowych informacji takich jak:
    - notatki służbowe;
    - podpięcie załączników w formie skanu jak innego dokumentu wykorzystywanego podczas redagowania wniosku;
14. Moduł powinien umożliwić przypisanie do dokumentu umowy dodatkowym informacji takich jak:
    - kontrahenta lub listy kontrahentów (przy wykorzystaniu danych zawartych w centralnej bazie systemu dziedzinowego);
    - podpięcie załączników w formie skanu jak innego dokumentu wykorzystywanego podczas redagowania projektu umowy;
    - formy oraz okresu zabezpieczenia umowy.
15. Moduł powinien być bezpośrednio związany z systemem finansowo – księgowym w taki sposób aby projekt umowy który zostanie zaakceptowany i zatwierdzony przez Skarbnika trafiał bezpośrednio do centralnego rejestru umów, w który to nastąpi dekretacja w/w dokumentu.
16. Moduł powinien umożliwiać wydruk procedowanych dokumentów zarówno w formie pojedynczej np. karta umowy, formularza wniosku zakupowego jak i w formie stosownych rejestrów.
17. Moduł powinien umożliwiać selektywne wyszukiwanie danych zgodnie z kryteriami:
    - Rodzaj procedury;
    - Numer sprawy

- Wydział zamawiający;
- Nazwa, opis zadania, przedsięwzięcia;
- Data dokumentu;
- Typ dokumentu;
- Okres realizacji umowy;
- Klasyfikacja i zadanie budżetowe;
- Kontrahent;
- Rodzaj oraz okres zabezpieczenia umowy;
- Kwota;
- Numer zewnętrzny;
- Numer wewnętrzny.

18. Moduł powinien posiadać funkcje pozwalające na przeprowadzenie procedur:
    - Anulowanie wniosku zakupowego;
    - Cofnięcie do wydziału zamawiającego;
    - Dokonanie aneksu do umowy;
    - Usunięcie projektu wniosku lub umowy.

Realizacja budżetu:

1. Moduł powinien być dostępny dla wszystkich jednostek organizacyjnych oraz pracowników wydziałów merytorycznych jednostki nadrzędnej.
2. Dostęp do wybranych obszarów budżetu powinno być realizowane poprzez określenie miejsca w strukturze organizacyjnej;
3. Moduł powinien umożliwić rejestrację wszystkich zatwierdzonych dokumentów stanowiących zaangażowanie środków RB.
4. Moduł powinien posiadać słownik typów rejestrowanych dokumentów.
5. Moduł powinien umożliwiać rejestrację dokumentów w oparciu o następujące pola danych:
    - Typ dokumentu;
    - Nazwa dokumentu;
    - Opis dokumentu;
    - Data na dokumencie;
    - Kontrahent;
    - Klasyfikacja i zadanie budżetowe
6. Moduł powinien umożliwiać weryfikację wprowadzonych danych z bieżącym stanem realizacji budżetu.
7. Moduł powinien sygnalizować o wszystkich przypadkach naruszenia dyscypliny budżetowej (przekroczenia wydatków)

7.4. System GIS – licencja szt. 1 – wymagania minimalne

Zadanie obejmuje dostarczenie pakietu zintegrowanych rozszerzeń w ramach istniejącego systemu GIS dedykowanych dla pracowników Zamawiającego do zarządzania rejestrami i informacją przestrzenną, umożliwiającej zarządzanie warstwami rastrowymi i wektorowymi, odczytywanie oraz tworzenie nowych danych, wykonywanie analiz przestrzennych, pomiarów, wyszukiwanie obiektów, odczytywanie załączników. Rozszerzenia wchodzące w skład pakietu muszą umożliwiać zarządzanie zasobami (w tym rejestrami) digitalizowanymi w ramach zamówienia. Zintegrowany charakter rozwiązania musi pozwalać użytkownikom na uzyskanie kompleksowej informacji dotyczącej wybranego terenu (gminy czy pojedynczej działki). Poszczególne rozszerzenia muszą pozwalać na elektronizację procesów związanych ze świadczeniem e-usług z zakresu informacji przestrzennej.

Rejestr Gminnej Ewidencji Zabytków

Rozszerzenie zawartości i funkcji w obrębie istniejącej aplikacji użytkowanej w urzędzie. Rozszerzenie powinno obejmować:

1. Zarządzanie bazą danych Gminnej Ewidencji Zabytków na terenie gminy,
2. Dodawanie obiektów punktowych, liniowych lub powierzchniowych poprzez zlokalizowanie obiektów w przestrzeni,

3. wprowadzenie obiektu w bazie danych przestrzennych poprzez ujawnienie pełnych informacji dotyczących zabytku,
4. Dla rejestru tabelarycznego zabytku nieruchomego powinien obejmować atrybuty w zakresie minimum wymaganym Rozporządzeniem Ministra Kultury i Dziedzictwa Narodowego z dnia 26 maja 2011 r. w sprawie prowadzenia rejestru zabytków, krajowej, wojewódzkiej i gminnej ewidencji zabytków oraz krajowego wykazu zabytków skradzionych lub wywiezionych za granicę niezgodnie z prawem. Szczegółowy zakres atrybutów zostanie uzgodniony z wykonawcą na etapie realizacji projektu,
5. Dla rejestru tabelarycznego zabytku archeologicznego powinien obejmować atrybuty w zakresie minimum wymaganym Rozporządzeniem Ministra Kultury i Dziedzictwa Narodowego z dnia 26 maja 2011 r. w sprawie prowadzenia rejestru zabytków, krajowej, wojewódzkiej i gminnej ewidencji zabytków oraz krajowego wykazu zabytków skradzionych lub wywiezionych za granicę niezgodnie z prawem. Szczegółowy zakres atrybutów zostanie uzgodniony z wykonawcą na etapie realizacji projektu,
6. Prezentacja obiektów rejestru w widoku mapy z zastosowaną odpowiednią stylizacją (klasyfikację obiektu) z etykietą, w odniesieniu do działek ewidencyjnych,
7. Przypisywanie załączników do konkretnych obiektów poprzez nazwanie załącznika i wskazanie lokalizacji pliku na dysku użytkownika. Można dodać załączniki w dowolnym formacie i liczbie,
8. Przypisywanie zdjęć aktualnych i archiwalnych do zabytku, przypisywanie mapy z położeniem stanowiska archeologicznego do obiektu,
9. Edycję i usuwanie wprowadzanych danych z poziomu widoku mapy lub tabeli,
10. Korzystanie ze słowników dla części atrybutów opisowych z możliwością ich edycji,
11. Przy dodawaniu nowego obiektu pobieranie oraz przypisanie części atrybutów opisowych z wcześniej dodanego obiektu oraz automatyczne wypełnianie danych zgodnie z rejestrem wynikających z relacji przestrzennych dodawanego obiektu,
12. Przeszukiwanie bazy danych zabytków i pozostałych danych zgromadzonych w rejestrze z możliwością przybliżania mapy do obiektu,
13. Wyszukiwanie obiektów poprzez wpisanie fragmentu dowolnej wartości zapisanej w module z opcją auto podpowiedzi tak, aby zapewnić wyszukiwanie z podaniem jedynie części szukanego ciągu znaków,
14. Filtrowanie oraz sortowanie obiektów z poziomu tabeli w obrębie każdego z pół, zaznaczanie obiektów poprzez narysowanie kształtu na mapie wraz z zaznaczeniem ich w tabeli oraz stosowanie filtrowania zaawansowanego,
15. Wybór pól widocznych w wybranym rejestrze oraz ustawienie sortowania po wskazanym polu rosnąco lub malejąco,
16. Przybliżanie okna mapy do wskazanego w tabeli rejestru obiektu,
17. Identyfikowanie obiektów na mapie poprzez ich wskazanie,
18. Edytowanie obiektu z poziomu tabeli,
19. Zapis wybranego rejestru do pliku xlsx, csv, shp, gml,
20. Tworzenie raportów, generowanie kart informacyjnych dla obiektu z możliwością zapisu ich do pliku na dysku,
21. Automatyczne generowanie karty zgodnie z Rozporządzeniem Ministra Kultury i Dziedzictwa Narodowego z dnia 26 maja 2011 r. w sprawie prowadzenia rejestru zabytków, krajowej, wojewódzkiej i gminnej ewidencji zabytków oraz krajowego wykazu zabytków skradzionych lub wywiezionych za granicę niezgodnie z prawem z możliwością wyboru do 4 zdjęć,
22. Generowanie załączników graficznych w oparciu o przygotowane kompozycje, dostosowanie wyglądu załącznika graficznego w postaci wyboru koloru poprzez wybór koloru z palety lub poprzez wpisanie wartości RGB, szerokości i odsunięcia obrysu działki oraz wyboru dostępnych warstw w projekcie, które będą widoczne na załączniku graficznym, dostosowywanie przeźroczystości oraz etykietowania obiektów,
23. Wyświetlanie treści rejestru w połączeniu z danymi dostępnymi w bazie danych przestrzennych w gminie np.: rejestr MPZP oraz danymi dostępnymi za pomocą usług sieciowych WMS i WFS m.in. dane GDOŚ dot. ochrony środowiska, ortofotomapa, BDOT10k,
24. Wyświetlanie treści rejestru na mapie z podkładem tematycznym m.in. z portali mapowych takich jak Open Street Map, Google Maps,

25. Obsługiwanie i uruchomienie wersjonowania obiektów w rejestrach z możliwością wyświetlania danych w określonych przedziałach czasowych.

7.5. e-edukacja – licencja szt. 1 – wymagania minimalne

System do planowania i zatwierdzania organizacji w jednostkach oświatowych (wraz z systemem raportowania)

System planowania i zatwierdzania organizacji (System) dostarcza jednostce samorządu terytorialnego funkcje ułatwiające gromadzenie, przechowywanie i przetwarzanie danych celem usprawnienia i przyspieszenia wykonywania codziennych obowiązków oraz uzyskania informacji umożliwiających podejmowanie optymalnych decyzji. Wspiera JST w obsłudze procesu planowania i zatwierdzania organizacji.

System:

1. korzysta z centralnego rejestru jednostek i użytkowników, w tym z centralnie definiowanej struktury jednostek sprawozdawczych;
2. jest wyposażony w centralne słowniki na potrzeby przygotowania projektu arkusza i projektu planu finansowego;
3. zapewnia na poziomie organu prowadzącego możliwość zatwierdzenia arkusza organizacyjnego przygotowanego w systemie oraz dalsze jego analizowanie.

System umożliwia:

1. centralne definiowanie warunków kontroli poprawnego opisu arkuszy przez dyrektora i sygnalizuje potencjalne nieprawidłowości w zakresie:
   - wymaganej liczebności oddziałów w zależności od typu szkoły,
   - liczebności grup na wybranych zajęciach (np. na zajęciach wychowania fizycznego, języków),
   - maksymalnych wymiarów etatów nauczycielskich w zależności od stanowiska (np. dyrektor, nauczyciel przedmiotu),
   - pensum bazowego dla wybranego stanowiska (np. bibliotekarza),
   - minimalnego stażu pedagogicznego;
2. prowadzenie niezależnych od arkusza rejestrów oddziałów, pracowników i przedmiotów na poziomie jednostki oświatowej tak, aby możliwe było śledzenie niezmienności planów nauczania oddziałów w kolejnych latach cyklu nauczania;
3. opisanie kwalifikacyjnych kursów zawodowych i innych zajęć kursowych;
4. opisanie zajęć międzyoddziałowych, pozalekcyjnych oraz innych zajęć edukacyjnych;
5. dokonywanie wyboru nauczyciela pełniącego funkcję wychowawcy i opiekuna stażu z istniejącej listy nauczycieli;
6. budowanie planu nauczania dla wybranego oddziału szkolnego, również na cały cykl kształcenia;
7. wskazanie miejsca prowadzenia zajęć (szczególnie istotne przy definiowaniu praktyk, warsztatów, zajęć pozaszkolnych itp.);
8. wprowadzenie opisu oddziałów o kilku zawodach i profilach kształcenia dla danego oddziału w szkołach ponadgimnazjalnych (tzw. oddziały wielozawodowe);
9. kopiowanie planów nauczania tak, aby można było wykorzystać raz zdefiniowany plan nauczania dla różnych oddziałów;
10. wskazanie w planie nauczania godzin do dyspozycji dyrektora, godzin JST;
11. definiowanie godzin realizowanych w układzie tygodniowym, semestralnym i rocznym;
12. budowę planów nauczania dla szkół działających w układzie semestralnym;
13. kontrolę zgodności planów nauczania poszczególnych oddziałów z planami ramowymi poza szkołami artystycznymi;
14. rejestrację danych pracowników jednostek oświatowych w zakresie niezbędnym do budowy arkusza oraz wyliczenia kosztów organizacji na potrzeby projektu planu finansowego;
15. definiowanie przydziałów czynności nauczycieli, w tym w podziale na grupy i w ramach grup międzyoddziałowych;
16. rejestrację kilku niezależnych umów nauczyciela w tej samej jednostce oświatowej;
17. automatyczne wyliczanie średniorocznych wymiarów etatów nauczycieli na podstawie przydzielonych zajęć, na podstawie pensum zajęć oraz okresu ich prowadzenia;
18. wyliczanie wymiarów etatu nauczycieli prowadzących zajęcia z różnych pensów na podstawie uśrednionego pensum definiowanego na poziomie umowy nauczycielskiej;
19. definiowanie przewidzianych przez przepisy zniżek obowiązkowego wymiaru godzin;

20. tworzenie wydruku projektu arkusza (dokument zatwierdzający i/lub tzw. płachty);
21. tworzenie aneksów do arkusza;
22. przygotowanie przez jednostkę oświatową arkusza na nowy rok szkolny poprzez wykorzystanie danych arkusza z poprzedniego roku szkolnego;
23. budowę kompletnego projektu planu finansowego w obszarze dochodów i wydatków budżetowych dla wszystkich typów jednostek oświatowych, w tym z możliwością przeliczenia kosztów związanych z realizacją planowanej organizacji z arkusza organizacyjnego;
24. na podstawie zgromadzonych danych przygotowywanie wydruków dla poszczególnych jednostek oświatowych, jak i zbiorczo:
    - projektu
    - wniosku o zmianę planu,
    - sprawozdań: Rb-27s, Rb-28s, Rb-Z, Rb-N, Rb-ZN, RB-UZ, Rb-NWS, Rb-27ZZ, Rb-50, Rb-34s,
    - sprawozdań finansowych: bilans, rachunek zysków i strat, zestawienie zmian w funduszu;
25. ułatwia automatyczną weryfikację poprawności sprawozdań budżetowych i sygnalizuje potencjalne nieprawidłowości. Mechanizm kontroluje powiązania pomiędzy poszczególnymi elementami sprawozdania Rb-27s i Rb-28s według następujących warunków:
    - dla wykonania dochodów:
        - Dochody wykonane + (należności pozostałe do zapłaty - nadpłaty) = należności,
    - dla wykonania wydatków:
        - Wydatki równe lub niższe niż plan,
        - Wydatki + zob. ogółem równe lub niższe niż plan,
        - Wydatki + zob. ogółem równe lub niższe niż zaangażowanie,
        - Zaangażowanie równe lub niższe niż plan albo równe lub wyższe od wydatków,
        - Zaangażowanie równe lub niższe niż plan.
26. umożliwia zbiorczą analizę zgromadzonych danych arkuszy organizacyjnych za pomocą MS Excel, w tym zapewniających możliwość analizy:
    - liczby uczniów / oddziałów w każdym typie placówek, rodzaju oddziału, specjalności,
    - nauczycielskich etatów przeliczeniowych w układzie jednostek oświatowych,
    - etatów losowych i etatów wsparcia,
    - specjalności nauczycieli,
    - zgodności przydziałów z kwalifikacjami,
    - zatrudnienia nauczycieli wg stopni awansu, pełnionych funkcji, nauczanych przedmiotów;

e-Pracownik

System umożliwia:

1. podgląd dla pracownika (po zalogowaniu) do kluczowych dla jego stosunku pracy informacji, w tym m.in.:
    - dane teleadresowe,
    - urlopy (przysługujący, planowany, wykorzystany) – przy jednoczesnym korzystaniu z systemu kadrowego
    - badania i szkolenia obowiązkowe do wykonania oraz wykonane – przy jednoczesnym korzystaniu z systemu kadrowego (Kadry VULCAN),
    - wynagrodzenie w formie pasków płacowych;
2. pobranie przez pracownika:
    - rocznej informacji dla osoby ubezpieczonej,
    - deklaracji podatkowej PIT-11,
    - ERP-7;
3. wypełnienie oraz wydrukowanie zestandaryzowanych formularzy niezbędnych do zatrudniania i bieżącej obsługi zatrudnienia bezpośrednio w wydzielonej i dostępnej dla pracowników części;
4. możliwość przekazania formularzy przez pracownika do działu kadr – przy jednoczesnym korzystaniu z systemu kadrowego (Kadry VULCAN);
5. przepływ wniosków urlopowych:
    - składanie wniosków urlopowych przez pracownika i przekazanie ich do akceptacji przełożonego,
    - akceptowanie lub odrzucanie wniosków urlopowych podwładnego przez przełożonego,

- przekazanie zaakceptowanego przez przełożonego wniosku do specjalisty ds. płac/kadr;

6. przepływ planów urlopowych:
   - składanie planów urlopowych przez pracownika i przekazanie ich do akceptacji przełożonego,
   - akceptowanie lub odrzucanie planów urlopowych podwładnego przez przełożonego,
   - przekazanie zaakceptowanego przez przełożonego wniosku do specjalisty ds. kadr – przy jednoczesnym korzystaniu z systemu kadrowego (Kadry VULCAN);
7. przepływ wniosków o wykonywanie pracy zdalnie:
   - składanie wniosków przez pracownika i przekazanie ich do akceptacji przełożonego,
   - akceptowanie lub odrzucanie wniosków podwładnego przez przełożonego,
   - przekazanie zaakceptowanego przez przełożonego wniosku do specjalisty ds. płac/kadr;
8. Informacja o wydanej odzieży roboczej wraz z planowanym terminem wymiany – przy jednoczesnym korzystaniu z systemu kadrowego (Kadry VULCAN);

Elektroniczny obieg listy płac

System umożliwia w pełni zelektryzowanie procesu podpisywania listy płac przez osoby sporządzające, zatwierdzające i sprawdzające je merytorycznie.

System umożliwia:

1. podpisywanie list płac z użyciem podpisu kwalifikowanego;
2. wskazanie osób, które składają podpis pod listami w poszczególnych jednostkach;
3. zdefiniowanie kolejności osób podpisujących listę płac;
4. otrzymywanie powiadomień mailowych o oczekujących na podpisanie list płac;
5. zdefiniowanie osób zastępujących w podpisywaniu listy.

Obsługa rekrutacji i przyjęć do szkół podstawowych

Oprogramowanie do rekrutacji wspiera pracowników JST, jednostek oświatowych oraz kandydatów i ich rodziców w procesie rekrutacji do żłobków, szkół i przedszkoli. W ramach systemu wyświetlana jest oferta dla kandydatów. Dodatkowo system umożliwia wprowadzenie informacji o osobach przyjmowanych do jednostek w innym trybie niż rekrutacja.

System umożliwia:

W zakresie dotyczącym naboru do szkół podstawowych

1. stworzenie i opublikowanie internetowego informatora o ofercie szkół podstawowych; informator musi składać się z wizytówek poszczególnych szkół;
2. definiowanie obwodów przez szkoły podstawowe w oparciu o dane TERYT;
3. import danych o dzieciach zameldowanych na terenie JST z systemu ewidencji ludności;
4. dostęp do informacji o przebiegu rekrutacji na każdym etapie rekrutacji dla organu prowadzącego oraz poszczególnych szkół podstawowych;
5. rodzicowi/opiekunowi prawnemu kandydata, użytkownikom ze szkół oraz organu prowadzącego dostęp do podręcznika użytkownika zawierającego informacje w zakresie obsługi systemu; podręcznik powinien być możliwy do pobrania w pliku PDF, aby użytkownik mógł z niego korzystać w dowolnym momencie;
6. dokonywanie przez organ prowadzący korekt w planie naboru w trakcie całego okresu trwania procedury rekrutacyjnej;
7. wypełnienie zgłoszenia do szkoły obwodowej lub wniosku o przyjęcie do szkoły podstawowej elektronicznie przy użyciu formularza na stronie internetowej, wydruk i złożenie papierowej wersji dokumentu lub przesłanie elektronicznego zgłoszenia lub wniosku po podpisaniu go podpisem elektronicznym (Profil Zaufany ePUAP lub podpis kwalifikowany);
8. dodanie do wniosku składanego elektronicznie załączników potwierdzających spełnianie przez kandydata kryteriów rekrutacyjnych poprzez wczytanie pliku ze skanem lub zdjęciem dokumentu;
9. opiekunowi samodzielne wpisanie hasła dostępu do konta;
10. organowi prowadzącemu na ustalanie wzoru wniosku o przyjęcie do szkoły;
11. automatyczne wskazanie szkoły obwodowej na podstawie adresu zamieszkania kandydata;
12. wskazanie przez opiekunów prawnych listy preferowanych szkół podstawowych (poza obwodowych), do których wnioskują o przyjęcie wraz z zaznaczeniem kolejności preferencji;

13. automatyczne przyjęcie do szkoły kandydatów z jej obwodu, których zgłoszenia zostały zaakceptowane;
14. dostęp do informacji o uczniach z obwodu oraz kandydatach spoza obwodu;
15. definiowanie stosowanych kryteriów naboru (w tym kryteriów automatycznych niewymagających wprowadzenia odpowiedzi przez osobę wypełniającą wniosek) oraz obliczanie liczby punktów z tytułu spełnienia określonych kryteriów określonych w zasadach rekrutacji;
16. organowi prowadzącemu przeprowadzenie serii próbnych przydziałów kandydatów, w trakcie których jest możliwość dokonywania zmian w planie naboru;
17. pobranie informacji w formie list o wynikach rekrutacji przez szkoły;
18. publikację wyników rekrutacji dla kandydatów za pośrednictwem Internetu;
19. zdalne potwierdzanie woli przez rodzica/opiekuna prawnego przy użyciu podpisu elektronicznego (Profil Zaufany ePUAP lub podpis kwalifikowany) lub za pomocą przesłanego skanu/zdjęcia z oświadczeniem;
20. powiadomienie kandydatów o statusie wniosku za pomocą poczty elektronicznej;
21. publikację na stronach internetowych informacji o pozostających wolnych miejscach;
22. przeprowadzenie procesu rekrutacji uzupełniającej, będącego powtórzeniem etapów rekrutacji właściwej;
23. wprowadzanie przez szkoły podstawowe informacji o kandydatach przyjmowanych do nich w ramach aktualizacji danych po zakończeniu procesu rekrutacji;
24. eksport list przyjętych w formacie *.SOU w celu zasilenia bazy programów uczniowskich;
25. organowi prowadzącemu kontrolę stanu wykonania prac na kolejnych etapach rekrutacji przez wszystkie uczestniczące w procesie jednostki;
26. spełnianie określonych obowiązującym prawem wymogów w zakresie ochrony danych osobowych.

System wspierający naliczanie opłat za pobyt i wyżywienie

System jest narzędziem służącym do prowadzenia naliczeń opłat ponoszonych przez rodziców dzieci uczęszczających do przedszkoli i szkół.

System umożliwia:

1. kontrolę dostępu do programu, ustalanie poziomu uprawnień użytkowników oraz haseł;
2. automatyczne tworzenie kopii bezpieczeństwa;
3. informacja i aktualizacja danych o dzieciach, rodzicach, jednostkach, grupach otrzymywana z dziennika elektronicznego;
4. szczegółowe ustawienia naliczania opłat ewidencjonowanych w przedszkolu:
   - opłaty za pobyt i/lub wyżywienie,
   - płatność „z góry”, „z dołu”,
   - możliwość ustawienie przypisów i odpisów;
5. dostęp do informacji o naliczeniach bieżących i archiwalnych – listy naliczeń;
6. dostarczenie informacji do witryny rodzica Dziennik VULCAN/aplikacji dzienniczek VULCAN o danych do przelewu dla rodzica;
7. zgłaszanie nieobecności możliwe z poziomu dziennika elektronicznego, witryny rodzica lub aplikacji dzienniczek VULCAN;
8. zgłaszanie nieobecności dziecka w wybranym dniu lub tygodniu dla pobytu i wyżywienia z poziomu samej aplikacji naliczającej opłaty;
9. podgląd do wszystkich zgłoszeń nieobecności i ilości godzin płatnych per dziecko
10. naliczanie opłat za pobyt i wyżywienie dziecka w przedszkolu oraz wyżywienia dla uczniów i pracowników;
11. naliczanie listy opłat dla instytucji dopłacających;
12. wprowadzenie ręczne wpłaty, umorzenia i zwrotu (w przypadku braku integracji z systemem księgowym VULCAN) lub pobranie danych automatycznie z systemu finansowego VULCAN (wpłaty, odsetki, umorzenia, status listy);
13. określanie zniżek i dofinansowania do pobytu i/lub wyżywienia;
14. stworzenie zestawienia opłat dla rodzica i jednostki;
15. wymianę danych z dziennikiem elektronicznym Dziennik VULCAN
16. pobranie danych z modułu stołówki o dietach;
17. przekazanie danych do modułu stołówki o zapotrzebowaniu na posiłki w danym dniu;

18. przekazanie danych do systemu finansowego (kontrahent, lista naliczeń, nr rachunku);
19. generowanie indywidualnego numeru rachunku bankowego dla płatności masowych;
20. możliwość wprowadzenia 5h godzin bezpłatnych dla pobytu w przedszkolu;
21. możliwość rozliczania godzinowego lub minutowego na pobycie;
22. możliwość wprowadzenia dodatkowego bezpłatnego czasu pobytu 15/30 minut na konkretne dziecko w przedszkolu (w celu np. obsłużenia bezpłatnej religii);
23. podział opłaty za wyżywienie na opłatę podstawową oraz dodatkową;
24. możliwość tworzenia osobnych cenników za wyżywienie dla przedszkolaków/uczniów/pracowników;
25. możliwość określenia obecności na wyżywieniu na podstawie pobytu.
26. Obsługa nieobecności płatnych

7.6. Obieg dokumentów – licencja szt. 50 – wymagania minimalne

Wymagania ogólne

1. EOD (Elektroniczny Obieg Dokumentów) musi realizować pełną funkcjonalność przewidzianą przepisami prawa dla systemu EZD.
2. EOD musi spełniać warunki określone dla systemu EZD w rozporządzeniu w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.
3. Jeśli jakaś czynność kancelaryjna jest obsługiwana przez EOD, to struktura systemu musi umożliwiać wykonywanie wszystkich wariantów tego zadania dopuszczalnych instrukcją kancelaryjną (np. dołączenie praktycznie dowolnej ilości dokumentów do sprawy – tzn. liczby na tyle dużej, by w praktyce nie napotkać ograniczeń systemu).
4. Moduły EOD muszą w szczególności:
   - umożliwiać rozproszoną rejestrację wszelkiej korespondencji każdego typu wpływającej do Zamawiającego wraz z załącznikami oraz jej automatycznym numerowaniem i tworzeniem raportów i zestawień
   - umożliwiać wielostronicowe skanowanie dokumentów z poziomu aplikacji oraz rejestrowanie ich
   - formy elektronicznej.
   - umożliwiać rejestrację i nadzorowanie obiegu korespondencji wewnętrznej Zamawiającego (pomiędzy pracownikami i komórkami organizacyjnymi)
   - udostępniać bazę nadawców i odbiorców korespondencji w celu sprawnej obsługi systemu i
   - przeglądania korespondencji wg nadawców i odbiorców dać możliwość wielopoziomowej dekretacji wpływającej korespondencji z możliwością niezależnego kierowania oryginałów dokumentów i sporządzania dowolnej ilości ich kopii, tworzonych na dowolnym etapie ich obiegu. Każda z utworzonych kopii dokumentów powinna być nadzorowana. Ponadto powinien EOD dać możliwość dekretacji dokumentów jedynie „do przeglądania”
   - rejestrować każdą czynność związaną z poszczególnym dokumentem, np. w postaci historii i dać
   - możliwość szybkiego odczytania tych informacji.
   - posiadać możliwość nadania poleceń i terminów realizacji związanych z korespondencją oraz ich kontroli
   - posiadać możliwość przydzielania zadań samemu sobie oraz innym użytkownikom zgodnie z przydzielonymi uprawnieniami oraz umożliwiać nadzorowanie terminu i sposobu realizacji
   - posiadać możliwość tworzenia i przeglądania zadań, poleceń, ponagleń, przypomnień przypisanych do wielu pracowników oraz powiązania ich z dokumentem lub sprawą.
   - posiadać możliwość udzielania zastępstw pracowników i pracy w zastępstwie
   - zapewniać jednoznaczne przypisanie odpowiedzialności za każdy z dokumentów
5. EOD musi być w pełni transakcyjny i musi zabezpieczać dane przed zniszczeniem lub przypadkowym nadpisaniem w przypadku równoczesnego korzystania z tych danych przez wielu użytkowników.
6. EOD od strony technicznej musi zapewnić skalowalność w zakresie wydajności, pojemności oraz dołączania dodatkowych użytkowników i elementów infrastruktury sprzętowej.

7. EOD musi zapewnić możliwość rozbudowy warstw poprzez zwiększenie zasobów komputerów obsługujących warstwę poprzez rozbudowę pamięci, zwiększenie liczby procesorów, zwiększanie liczby maszyn oraz zwiększenie pojemności pamięci masowych.
8. EOD musi umożliwiać rozpraszanie repozytorium dokumentów w ramach jednego systemu elektronicznego obiegu dokumentów na wiele baz danych w różnych lokalizacjach (np. budynki urzędu, serwerownie).
9. EOD musi być zgodny z przepisami prawa, obowiązującymi na dzień ostatecznego odbioru systemu.
10. EOD musi posiadać mechanizm kontroli dostępu do usług pozwalający na dostęp do danej usługi ze względu na użytkownika oraz grupę (jednostkę organizacyjną) do której należy.
11. System musi być wyposażony w komunikator, pozwalający na wymianę wiadomości tekstowych w czasie rzeczywistym. Komunikator systemowy powinien zapewniać wymianę wiadomości zarówno między użytkownikami systemu jak i przekazywanie użytkownikowi komunikatów przez system.
12. EOD musi umożliwić wprowadzanie zmian kadrowych, urlopów i zastępstw bez konieczności modyfikacji ścieżek procedowania i umożliwia przekazanie osobie zastępującej części lub całości uprawnień osoby zastępowanej. Uprawnienia muszą być przekazane na określony czas.

Administracja i konfiguracja, raportowanie

1. EOD musi umożliwić definiowanie i wykorzystywanie wartości domyślnych dla wybranych pól w formularzach opisujących dokumenty, sprawy oraz sposób ich przetwarzania, tam gdzie wykorzystanie ustawień domyślnych znacznie usprawni pracę. Ustalenie takiej konfiguracji powinno być możliwe zarówno globalnie dla całego systemu, jak i na poziomie użytkownika.
2. EOD musi pozwalać na dodawanie dodatkowych metadanych dla pism, spraw, teczek, interesantów, zadań (tekst, słownik, data i godzina, wartość z e-formularzy ePUAP) z możliwością wykorzystania ich na listach, raportach, serwisach komunikacyjnych.
3. EOD będzie umożliwiał wykorzystanie skrótów klawiszowych do wywoływania często użytkowanych funkcji. EOD będzie zawierał zestaw predefiniowanych skrótów klawiszowych i umożliwi zdefiniowanie własnych na poziomie głównego menu systemu.
4. EOD musi posiadać jednolity i przejrzysty interfejs graficzny dla każdego z modułów. System powinien w sposób czytelny pokazywać poszczególne etapy obiegu dokumentów oraz mieć możliwość wprowadzenia struktury organizacyjnej urzędu (schematu organizacyjnego).
5. EOD musi umożliwiać odwzorowanie wieloszczeblowej struktury organizacyjnej Zamawiającego z możliwością jej dowolnej modyfikacji. Struktura powinna umożliwiać definiowanie: jednostek organizacyjnych, komórek organizacyjnych, pracowników zatrudnionych w komórkach, ich funkcje i stanowiska.
6. EOD umożliwi tworzenie grup użytkowników, definiowanie ich uprawnień do wykonywania funkcji oraz definiowanie uprawnień każdego z pracowników w zakresie: dostępu do dokumentów i spraw oraz uprawnień do aktualizacji i przeglądania ich zawartości. Możliwe powinno też być kopiowanie uprawnień użytkowników.
7. EOD musi umożliwić ewidencjonowanie struktury instytucji oraz jej pracowników, które umożliwią przypisanie pracowników (osób) do stanowisk (funkcji).
8. EOD umożliwi zarządzanie uprawnieniami w oparciu o grupy uprawnień i dostępnych zasobów, jakich dotyczą. System uprawnień musi być zdolny do odzwierciedlenia uprawnień i odpowiedzialności poszczególnych urzędników, stosowany w jednostkach samorządu terytorialnego i wynikający z Instrukcji Kancelaryjnych oraz struktury jednostki.
9. System powinien rejestrować historię zmian dokonywanych w strukturze organizacyjnej i uprawnieniach oraz umożliwiać dostęp do archiwalnych zapisów struktury organizacyjnej.
10. W zakresie obsługi wzorców dokumentów EOD musi zapewniać definiowanie szablonów w formacie RTF z poziomu systemu z możliwością wstawiania do treści pisma znaczników, których zawartość jest automatycznie odczytywana z bazy danych dokumentów, interesantów i kontrahentów. System powinien zapewnić automatyczne wstawianie minimum następujących danych do treści pisma:
    - Danych adresata (minimum: nazwisko, imię, instytucję, kod pocztowy, nazwę miejscowości, nazwę ulicy, numer domu i lokalu),
    - Danych strony zainteresowanej (minimum: nazwisko, imię, instytucję, kod pocztowy, nazwę miejscowości, nazwę ulicy, numer domu i lokalu),

- Tematu dokumentu,
- Numeru dokumentu,
- Znaku sprawy z którą dokument jest związany,
- Datę utworzenia,
- Dane autora dokumentu,
- Symbol komórki organizacyjnej autora dokumentu,
- Możliwość łączenia szablonów w grupy i podgrupy.
- Możliwość definiowania szablonów do wydruku kopert

11. EOD musi posiadać wbudowany mechanizm zdalnej asysty technicznej pozwalający na wsparcie użytkowników systemu przez uprawnionych do tego administratorów.
12. EOD umożliwia administratorowi wymuszenie okresowej zmiany haseł oraz określenie polityki dotyczącej „siły" hasła. Hasła powinny być przechowywane w systemie w formie zaszyfrowanej i nie ma możliwości ich odtworzenia, lecz jedynie zresetowania. Po zresetowaniu hasła użytkownika przez administratora systemu zmusza użytkownika do wprowadzenia nowego hasła przy pierwszym logowaniu
13. Słowniki prowadzone i wykorzystywane w systemie EOD muszą obejmować w szczególności: JRWA, słownik typów dokumentów i spraw, słownik lokalizacji, słownik rodzajów nośników, słownik kategorii archiwalnych. Wymagane jest aby pola zawierające powtarzalne dane miały możliwość wypełniania ich za pomocą słowników systemowych. W zakresie obsługi słowników wspomagających wypełnianie pól tekstowych użytkownicy powinni mieć możliwość tworzenia indywidualnych słowników z wpisami dostępnymi tylko dla danego użytkownika.
14. System powinien mieć możliwość wprowadzenie śledzenia historii zmian dla pól metadanych związanych z opisem dokumentu. Historia ta powinna obejmować informacje o zawartości danego pola przed i po zmianie, dacie zmiany oraz osobie jej dokonującej.
15. EOD musi umożliwić definiowanie sposobu logowania dla poszczególnych użytkowników. Dostępne muszą być co najmniej następujące metody logowania: użytkownik/hasło, logowania przez domenę.
16. EOD musi umożliwić nadawanie i ograniczanie uprawnień do danych osobowych interesantów – osób fizycznych, zapewniając ochronę tych danych zgodnie z ustawą o ochronie danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).
17. EOD musi umożliwić zdefiniowanie dodatkowych metadanych do opisu spraw oraz dokumentów.
18. Wymaga się, aby była możliwość dowolnego ustawiania kolumn oraz zapamiętywania tych ustawień. Funkcjonalność ta musi obejmować wyświetlania bądź ukrywanie kolumn na wyświetlanych listach w systemie EOD. Wymaga się, aby była możliwość wykorzystania na listach mechanizmów szybkiej filtracji oraz wyszukiwania po dowolnie wybranej kolumnie.

Rejestracja i procedowanie dokumentów oraz teczek spraw

1. EOD musi obsługiwać rejestrację przesyłek przychodzących w formie papierowej (składane osobiście, przysyłane pocztą) i elektronicznej (składane osobiście na nośnikach, przesyłane przez elektroniczną skrzynkę podawczą oraz pocztą elektroniczną) wraz z załącznikami zgodnie z wymogami Rozporządzenia w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r. Nr 14, poz. 67).
2. W ramach procesu rejestracji przesyłek przychodzących w formie papierowej EOD musi umożliwić zeskanowanie (z poziomu interfejsu aplikacji) poszczególnych dokumentów, wchodzących w skład przesyłki.
3. EOD musi umożliwiać generowanie potwierdzenia przyjęcia przesyłki przychodzącej przez punk kancelaryjny.
4. EOD musi umożliwiać rejestrację przesyłek w wielu punktach kancelaryjnych.
5. EOD musi umożliwiać opatrywanie przesyłek przychodzących metadanymi zgodnie z obowiązującymi przepisami oraz dodatkowymi (konfigurowalny zakres), przy czym metadane powinny być słownikowane co najmniej w zakresie rodzaju dokumentu, rejestru oraz danych teleadresowych.
6. EOD musi umożliwić odróżnienie i jednoznaczną identyfikację dokumentów, przechowywanych w postaci skanów, wchodzących w skład przesyłki, przy zachowaniu ich powiązania z przesyłką.

7. Dla dokumentów papierowych nie podlegających skanowaniu oraz dokumentów na nośnikach elektronicznych nie podlegających kopiowaniu do systemu EOD musi być możliwe sporządzenie metryki, zawierającej podstawowe informacje o dokumencie (co najmniej – tytuł, identyfikator, notatka).
8. EOD musi umożliwić prawidłową obsługę przychodzącej poczty elektronicznej, zgodnie z wymogami przepisów w zakresie instrukcji kancelaryjnych (rejestracja w rejestrze przesyłek wpływających lub bezpośrednie dołączenie wiadomości z załącznikami do akt sprawy)
9. EOD musi automatycznie pobierać przesyłki, które przyszły przez elektroniczną skrzynkę podawczą systemu ePUAP oraz skrzynkę e-Doręczeń, i musi umożliwić ich rejestrację w systemie. Dokumenty powinny otrzymywać określone typy a wybrane dane z formularzy elektronicznych powinny być przepisane do metadanych zapisywanych w systemie.
10. EOD musi umożliwić generowanie i drukowanie nalepek z kodami kreskowymi na dokumenty papierowe oraz nośniki i odnajdywanie na podstawie zeskanowanej nalepki odwzorowania cyfrowego danego dokumentu
11. Rozdział przesyłek przychodzących do właściwych komórek merytorycznych i pracowników musi się odbywać poprzez przekazanie uprawnień do dokumentów i informacji zawartych w systemie.
12. EOD musi umożliwić rejestrację obiegu (lokalizacja, czas przemieszczenia, użytkownik, potwierdzenie odbioru) dokumentów dla których istnieje odwzorowanie cyfrowe oraz dla których nie zostało ono wykonane.
13. EOD musi umożliwić sporządzanie odwzorowań cyfrowych dokumentów poprzez skanowanie dostępne bezpośrednio z poziomu aplikacji, zgodnie z wymaganiami określonymi w instrukcji kancelaryjnej.
14. EOD musi umożliwić rejestrację, przechowywanie, procedowanie oraz dołączanie do akt sprawy dokumentów elektronicznych, dokumentów papierowych w postaci odwzorowań, jak również metryk (dla dokumentów papierowych nie skanowanych i elektronicznych na nośnikach).
15. EOD musi umożliwić wszczynanie, prowadzenie i załatwianie spraw, przechowywanie akt sprawy i prowadzenie spisów spraw zgodnie z obowiązującymi przepisami. EOD automatycznie musi nadawać znak sprawy i zapewnia jego zgodność z wymogami instrukcji kancelaryjnej.
16. EOD musi umożliwiać ręczne przenumerowanie sprawy w przypadkach dopuszczonych instrukcją kancelaryjną.
17. EOD musi umożliwić prowadzenie rejestrów kancelaryjnych, w tym rejestru przesyłek wpływających, wychodzących oraz pism wewnętrznych, definiowanie i prowadzenie dowolnych innych rejestrów kancelaryjnych dopuszczonych instrukcją kancelaryjną. W przypadku dokumentów wewnętrznych i wychodzących system powinien umożliwić tworzenie indywidualnych rejestrów dla poszczególnych pracowników i automatycznie przydzielać do nich te dokumenty.
18. EOD musi umożliwić numerację i klasyfikację pism oraz spraw w oparciu o JRWA zgodnie z instrukcją kancelaryjną.
19. EOD musi od strony technicznej musi umożliwić stworzenie podrzędnych jednostek podległych i odrębna podległość w strukturze organizacyjnej.
20. EOD musi umożliwić procedowanie i dekretację spraw oraz pism z wykorzystaniem mechanizmu procedowania według definiowalnych ścieżek. Akceptacja dokumentów z wykorzystaniem mechanizmu procedowania według zdefiniowanej ścieżki powinna być jedno lub wielostopniowa.
21. Akceptacja pism elektronicznych przeznaczonych do wysyłki musi się odbywać z wykorzystaniem podpisu elektronicznego zgodnie z wymogami prawa.
22. EOD musi umożliwić zapis projektów pism przekazywanych pomiędzy użytkownikami w trakcie załatwiania sprawy, a także zamieszczanie adnotacji odnoszących się do projektów pism. System powinien zapisywać wszystkie wersje dokumentu i umożliwiać ich przeglądanie z informacją o użytkowniku, który zapisał daną wersję oraz dacie jego utworzenia. Skierowanie danego dokumentu na rejestr pism wychodzących powoduje umieszczenie na nim wersji ostatecznej dokumentu a jego dalsza modyfikacja nie jest możliwa.
23. EOD musi zapewnić prowadzenie i wydruk metryki sprawy zgodnie z obowiązującymi przepisami.

24. EOD musi umożliwić opisywanie spraw i akt sprawy metadanymi zgodnie z obowiązującymi przepisami.
25. EOD ma umożliwiać wiązanie dowolnych dokumentów ze sobą oraz ze sprawami oraz dodawanie do nich adnotacji i przypomnień.
26. EOD musi umożliwić zarządzanie składami chronologicznymi i składami informatycznych nośników danych.
27. EOD musi umożliwić sporządzanie i wydruk raportów, statystyk i zestawień, w szczególności wymaganych przepisami prawa. EOD umożliwi monitorowanie liczby spraw i terminowości ich załatwiania (globalnie, przez poszczególne komórki i osoby) w zadanych przedziałach czasu, także w podziale na kategorie spraw. Możliwość generowania raportów będzie zależna od uprawnień i będzie dotyczyła pracy osób i komórek podległych oraz pracy osoby sporządzającej raport.
28. EOD musi umożliwić użytkownikowi dostęp do zestawienia spraw i dokumentów, za które jest odpowiedzialny, zestawienia aktualnych zadań wynikających z przepływu pracy (sprawy i korespondencja, w odniesieniu do których użytkownik ma aktualnie coś do zrobienia), zestawienia korespondencji otrzymanej i wysłanej. Dodatkowo EOD musi wydzielić automatycznie w wizualizacji niezałatwione sprawy, których zbliża się termin realizacji zgodnie z ustawionym przez administratora kryterium ilości dni pozostałych do realizacji.
29. EOD musi posiadać funkcję umieszczania pisma na rejestr dokumentów przeznaczonych do wysłania na platformę ePUAP oraz za pośrednictwem eDoręczeń.
30. EOD musi umożliwić automatyczną wysyłkę korespondencji pocztą elektroniczną poprzez pobranie adresu odbiorcy i wysłanie pisma/pism w formie załączników do poczty. Wysyłanie powinno być realizowane w pojedynczym e-mailu zarówno w odniesieniu do dokumentu jaki i całej teczki sprawy. Treść e-maila oraz zakres dołączanych dokumentów w formie załączników powinna być dostępna do edycji dla użytkownika odpowiedzialnego za realizacje wysyłki.
31. EOD musi umożliwić odnotowanie wysyłki wszelkich przesyłek wychodzących w rejestrze i opatrzenie ich metadanymi zgodnie z przepisami. EOD będzie w miarę możliwości automatyzował te czynności.
32. EOD musi umożliwić generowanie korespondencji seryjnej i automatyzację jej wysyłki (do zdefiniowanych, konfigurowalnych grup odbiorców).
33. EOD musi umożliwić użytkownikowi podgląd przypisanych do niego spraw i korespondencji, z możliwością sortowania, filtrowania i przeszukiwania oraz wizualizacji spraw pilnych do realizacji oraz przeterminowanych. Wizualizacja spraw pilnych i przeterminowanych ta powinna być dokonywana automatycznie.
34. EOD musi zapewnić przydzielanie spraw i korespondencji konkretnym użytkownikom pracującym na danym stanowisku. Przekazywanie dokumentów lub spraw do wskazanego Użytkownika musi wymagać odnotowania potwierdzenia faktu tego przekazania i zapisania go w systemie. Przekazanie teczki sprawy odbywa się wraz z całą dokumentacją do niej przynależną. System powinien umożliwić także przekazanie teczki sprawy z dostępem tylko do części dokumentów oraz możliwością określenia zakresu w jakim dany Użytkownik może przetwarzać dokumenty (podgląd lub edycja/ wersjonowanie dokumentu).
35. EOD musi zapewnić możliwość równoczesnego dostępu do dokumentacji wielu użytkownikom wraz z możliwością wspólnej pracy w zakresie gromadzenia akt danej sprawy.
36. EOD musi umożliwić składanie i weryfikowanie podpisu elektronicznego.
37. EOD musi posiadać edytor, służący do sporządzania notatek załączanych do akt sprawy.
38. EOD musi umożliwić tworzenie i obsługę sposobów procedowania spraw i obiegu dokumentów. W szczególności EOD musi umożliwić zdefiniowanie ścieżki przebiegu procedowania, która zaczyna się i kończy w określonym węźle. Definicje muszą dopuszczać rozwidlanie oraz łączenie się ścieżek (ścieżek w obrębie innych ścieżek) i określenie dokumentów wymaganych na danym procesie procedowania.
39. Modelowanie ścieżek musi odbywać się w narzędziu graficznym a procedowanie sprawy wg. zdefiniowanej ścieżki realizacji powinno się zwizualizować w postaci graficznej tożsamej z procesem modelowania.
40. EOD musi umożliwić przypisywanie procesom (realizowanym w ramach ścieżki lub „ad-hoc") terminów realizacji, osób odpowiedzialnych za wykonanie poszczególnego etapu oraz osób nadzorujących dany etap. Nadzór oraz odpowiedzialność za realizację powinna być też

wymagana w odniesieniu do całego procesu. Osoby nadzorujące dany proces (lub jego etap) powinny mieć na swoim koncie bezpośredni wgląd w postęp realizacji danej procedury z uwzględnieniem jego terminowości bez konieczności wywoływania dodatkowych funkcji.

41. EOD musi umożliwić procedowanie sprawy lub korespondencji trybem „ad hoc" poprzez określanie na bieżąco kolejnych stanowisk zajmujących się sprawą/dokumentem bez wykorzystywania uprzednio zdefiniowanych ścieżek procedowania sprawy/dokumentu. Użytkownik może przejść do trybu „ad hoc" w dowolnym momencie procedowania.
42. EOD musi umożliwić ewidencjonowanie i grupowanie zdefiniowanych ścieżek obiegu.
43. EOD musi umożliwić przeszukiwanie i sortowanie pism i spraw w szczególności wg znaku sprawy, identyfikatora przesyłki, osoby lub komórki odpowiedzialnej, kategorii JRWA, dat wpłynięcia lub załatwienia, terminu załatwienia, statusu pisma lub sprawy, danych petenta.
44. EOD musi umożliwić obsługę plików (dokumentów) w dowolnym formacie zgodnym z obowiązującymi przepisami prawa (pliki te są otwierane i modyfikowane przez użytkowników w odrębnych aplikacjach).
45. W zakresie obsługi archiwum zakładowego EOD musi zapewnić automatyczne przejmowanie dokumentacji przez archiwum zakładowe po upływie okresu przewidzianego w instrukcji kancelaryjnej. Przejęcie dokumentacji musi polegać na przekazaniu archiwiście uprawnień do tej dokumentacji w systemie EOD i ograniczeniu uprawnień komórki merytorycznej, zgodnie z instrukcją kancelaryjną.
46. W zakresie obsługi archiwum zakładowego EOD musi posiadać dedykowane funkcje do udostępniania i wycofywania dokumentacji elektronicznej z archiwum zakładowego.
47. W zakresie obsługi archiwum zakładowego EOD musi realizować brakowanie akt elektronicznych oraz przekazanie akt do archiwum państwowego. System musi zapewnić typowanie dokumentacji do brakowania lub przekazania do archiwum państwowego po upływie terminów związanych z danymi kategoriami archiwalnymi.
48. W zakresie obsługi archiwum zakładowego EOD musi zapewnić wsparcie dla procesu archiwizacji informatycznych nośników danych oraz dokumentów papierowych dla których nie wykonano pełnego odwzorowania cyfrowego poprzez sporządzanie spisu zdawczo-odbiorczego, zapis miejsca ich przechowywania i kategorii archiwalnej, wsparcie procedury brakowania akt oraz wypożyczania oraz przekazania do archiwum państwowego

Integracje i interfejsy, współpraca z platformą ePUAP i e-Doręczeniami

1. EOD musi rejestrować wszystkie czynności dostępu do usług i zasobów w systemie, w zakresie dostępu przez użytkowników oraz aplikacje współpracujące z EOD.
2. EOD powinien posiadać interfejsy komunikacyjne umożliwiające jego integrację z innymi systemami w zakresie wymiany informacji z internetowymi platformami urzędu oraz systemami dziedzinowymi..
3. Interfejsy komunikacyjne muszą być oparte w oparciu o serwisy komunikacyjne Web Services. Ustandaryzowane interfejsy zewnętrzne, powinny udostępniać usług integracyjnych zapewniające systemom zewnętrznym poprzez usługi Web Services minimum w oparciu o standardy SOAP 1.2, WSDL co najmniej 1.1, możliwość komunikacji z wykorzystaniem plików XML (standard XML 1.0 i XSD 1.1).
4. Opracowane mechanizmy integracyjne muszą umożliwiać wymianę danych pomiędzy:
   - systemami dziedzinowymi urzędu
   - platformami internetowymi urzędu
   - platformą e-PUAP
5. Mechanizmy integracyjne w zakresie systemu EOD muszą umożliwiać
   - rejestrację dokumentu w systemie EOD
   - rejestracje teczki spraw w EOD zgodnie z Jednolitym Rzeczowym Wykazem Akt
   - umieszczenie dokumentu w wybranej teczce na podstawie numeru sprawy
   - integracja kartotek petentów w zakresie dodawanie nowej osoby, importu danych personalnych z kartotek EOD
   - pobierania dokumentów z EOD wraz z metadanymi pozwalającymi w minimalnym zakresie na określenie daty jego powstania, identyfikacji petentów z nim powiązanych, numeru teczki sprawy w której się ten dokument znajduje, daty wprowadzenia na rejestr korespondencji przychodzącej lub daty wysłania dokumentu do petenta (w przypadku korespondencji poleconej daty potwierdzenia odbioru), terminów płatności dla

dokumentów finansowych, identyfikacji osoby prowadzącej daną sprawę, inne metadane związane z typem dokumentu wprowadzane do systemu EOD oraz połączone z dokumentem jego cyfrowe odwzorowania lub dokumenty w wersji elektronicznej
- pobieranie informacji o teczkach spraw w zakresie numeru sprawy, daty rejestracji, wymaganego terminu realizacji, daty załatwienia sprawy, osoby odpowiedzialnej, listy dokumentów w obrębie teczki, statusu stanu sprawy, inne dane związane z realizacją sprawy

6. W zakresie wymiany danych pomiędzy systemami dziedzinowymi a EOD opracowane mechanizmy integracyjne muszą co najmniej umożliwiać :
   - automatyczne przekazywanie dokumentów tworzonych w modułach dziedzinowych wraz z automatycznym dodawaniem ich do teczek spraw bezpośrednio w systemie EOD.
   - synchronizację kartotek kontrahentów na poziomie modułów dziedzinowych i systemu EOD zapewniając dwukierunkową wymianę metadanych dokumentów.
7. W zakresie wymiany danych pomiędzy systemem EOD a platformą e-PUAP a systemami dziedzinowymi opracowane mechanizmy integracyjne muszą co najmniej umożliwiać wykonanie następujących operacji :
   - EOD musi przyjmować dokumenty elektroniczne złożone przez klientów za pośrednictwem platformy ePUAP lub za pośrednictwem e-Doreczenia i umożliwiać kierowanie ich na właściwą ścieżkę realizacji dla wybranej procedury.
   - EOD musi umożliwiać doręczanie petentom dokumentów poprzez elektroniczną skrzynkę podawczą platformy ePUAP oraz za pośrednictwem e-Doreczenia.
   - EOD powinien umożliwić wysyłkę wybranego dokumentu do określone grupy odbiorców na ich skrytki na platformie ePUAP oraz za pośrednictwem e-Doreczenia.
   - Rejestracja dokumentu przekazanego z platformy ePUAP lub e-Doręczenia posiadającego załączniki powinna obejmować ich wizualizację bezpośrednio w systemie obiegu dokumentów.
     EOD musi realizować pełną obsługę wysłania i odbioru dokumentów przesyłanych za pośrednictwem platformy ePUAP i e-Doręczenia.

7.7. Monitoring środowiska – zestaw. 1 – wymagania minimalne

Pozycja dotyczy wdrożenia systemu monitoringu środowiskowego obejmującego bieżące pomiary następujących czynników szkodliwych: PM2,5, PM10, PM1 w lokalizacjach na terenie powiatu. Dodatkowo prowadzone będą pomiary temperatury, wilgotności, ciśnienia atmosferycznego. Dane zbierane z czujników publikowane będą na portalu eBOM oraz będą udostępniane w formie danych surowych, otwartych wszystkim zainteresowanym stronom. Przewiduje się udostępnienie danych okresowych na portalu eBOM. System składał się będzie z trzech (3) stacji pomiarowych oraz zintegrowanego z nimi systemu informatycznego (aplikacja dostępna w chmurze) zapewniającego ich analizę i publikację. Ponadto dane z czujników będą prezentowane w ujęciu geograficznym na podkładach mapowych.

Urządzenie pomiarowe/czujniki zapewnią pomiary:
- temperatury w zakresach przynajmniej od -30 °C do +60°C oraz dokładnością co najmniej 0,5'C;
- wilgotności powietrza przynajmniej w zakresach od 0-100 % wilgotności względnej przy dokładności ±3%;
- ciśnienia atmosferycznego nad poziomem morza, przeliczony z wartości podawanych przez urządzenie z uwzględnieniem wysokości na jakiej zostanie zamontowany – zakres min. 700-1200hPa oraz dokładności 1 hPa
- pyłu zawieszonego PM1.0 w zakresie pomiarowym 0 – 500 µg/m^3 z dokładnością pomiarową ±10 µg/m^3;
- pyłu zawieszonego PM2.5 w zakresie pomiarowym 0 – 1000 µg/m^3 z dokładnością pomiarową ±10%;
- pyłu zawieszonego PM10 w zakresie pomiarowym 0 – 1000 µg/m^3 z dokładnością pomiarową ±10%;

System pomiaru obejmował będzie czujniki do pomiaru jakości powietrza, system monitorowania w postaci platformy informacyjnej wizualizującej wyniki pomiarów w czasie rzeczywistym oraz aplikacji

mobilnej. Systemy dostępne w wielu wersjach językowych. W ramach projektu założono instalację 3 punktów pomiarowych.

Czujniki do pomiaru jakości powietrza

1. Komunikacja z serwerem wykonawcy gromadzącym i udostępniającym informacje z czujników za pomocą sieci GSM.
2. Urządzenie pomiarowe/czujniki zapewnią pomiary:
   - temperatury w zakresach przynajmniej od -40 °C do +80°C oraz dokładnością co najmniej 0,5'C;
   - wilgotności powietrza przynajmniej w zakresach od 0-100 % wilgotności względnej przy dokładności ±3%;
   - ciśnienia atmosferycznego nad poziomem morza, przeliczony z wartości podawanych przez urządzenie z uwzględnieniem wysokości na jakiej zostanie zamontowany – zakres min. 700-1200hPa, dokładność 1 hPa;
   - pyłu zawieszonego PM 1.0 w zakresie pomiarowym 0 – 500 µg/m³ z dokładnością pomiarową ±10 µg/m³;
   - pyłu zawieszonego PM2.5 w zakresie pomiarowym 0 – 1000 µg/m³ z dokładnością pomiarową ±10 µg/m³;
   - pyłu zawieszonego PM10 w zakresie pomiarowym 0 – 1000 µg/m³ z dokładnością pomiarową ±10 µg/m³;
3. Urządzenia muszą wykazywać niepewność wskazań średnich dobowych stężenia pomiędzy dwoma urządzeniami na poziomie maksimum 10% dla pyłów PM2.5 i PM10.
4. Sensory muszą zostać poddane, przed ich montażem oraz w czasie ich eksploatacji, kalibrowaniu z urządzeniem posiadającym wykazaną równoważność do metody referencyjnej badań pyłu zawieszonego w powietrzu.
5. Urządzenia muszą posiadać zasilanie z sieci energetycznej 230V/110V i posiadać kabel zasilający o długości min. 2.5 metra wyposażony w USB lub wtyczkę sieciową.
6. Urządzenia muszą zostać zamontowane w sposób nieinwazyjny, zapewniający brak ingerencji w elewację czy też inne elementy budynków np. elewację i stolarkę okienną/drzwiową.
7. Urządzenia muszą posiadać możliwość przeniesienia do innej lokalizacji.
8. Urządzenia muszą posiadać min. 36-miesięczną gwarancję sprzętową na całość urządzeń pomiarowych.
9. Urządzenia muszą posiadać wbudowany system powiadamiania kolorem diody w zależności od stanu jakości powietrza. Kolory wyświetlane na diodach czujnika muszą być kompatybilne z tymi wyświetlanymi na platformie internetowej i w aplikacjach mobilnych.
10. Urządzenia powinny posiadać system podgrzewania powietrza przed pomiarem w celu wyeliminowanie wpływu wilgotności na pomiary stężenia pyłów w powietrzu. W konstrukcji urządzenia musi zostać przewidziany element kondycjonujący próbkę powietrza przed pomiarem, w celu podgrzania jej powyżej punktu rosy.
11. Urządzenia powinny zapewniać stopień ochrony na poziomie min IP 34. Obudowa urządzenia musi być odporna na warunki zewnętrzne i być przystosowana do pracy w trudnych warunkach atmosferycznych. Wskazana obudowa z aluminium, stali nierdzewnej itp.
12. Temperatura pracy urządzeń musi wynosić przynajmniej od -40 °C do +80°C.
13. Maksymalny pobór mocy czujnika to max 2,5 W
14. Roczny pobór mocy nie może przekraczać 11 kWh.
15. Urządzenie powinno być przeznaczone do montowania na wysokości od 1,5 do 8 metrów nad poziomem ziemi.
16. Masa urządzenia nie może być większa niż 500 gram ze względu na planowane miejsce instalacji urządzeń.
17. Wymiary urządzenia nie mogą być większe niż 140/140/140 mm nie licząc ewentualnej zewnętrznej anteny nadawczej ze względu na planowane miejsce instalacji urządzeń.

Systemu monitorowania jakości powietrza:

1. Wykonawca zapewni bezpłatny dostęp do ogólnodostępnej platformy informacyjnej wizualizującej wyniki pomiarów w czasie rzeczywistym. Platforma internetowa musi być obsługiwana w polskiej i angielskiej wersji językowej.
2. Platforma musi być dostosowana dla osób niepełnosprawnych (słabowidzących, osób z dysfunkcją wzrokową)

3. Dane pomiarowe (PM1, PM2.5, PM10, temperatura, wilgotność, ciśnienie) muszą być aktualizowane minimum co 5 minut i wizualizowane na platformie internetowej oraz w aplikacji mobilnej.
4. Wykonawca zapewni darmową aplikację mobilną, prezentującą wyniki pomiarów w czasie rzeczywistym dostępne dla minimum 2 systemów operacyjnych: Android (Google Play) i IOS (App Store) z zasięgiem przynajmniej ogólnopolskim. Aplikacja mobilna musi być obsługiwana w polskiej i angielskiej wersji językowej.
5. Wykonawca zapewni dostęp do widget-u pozwalającego na publikację danych na wskazanych przez Zamawiającego stronach www.
6. Platforma internetowa oraz aplikacja mobilna musi zapewnić dane pomiarowe dotyczące pyłów PM1, PM2.5, PM10 oraz dane pogodowe: temperatura, wilgotność, ciśnienie i siła wiatru.
7. Dane z sensorów (dane pomiarowe) muszą być zgodne z europejskim wskaźnikiem jakości powietrza CAQI (Common Air Quality Index). Prezentacja tych danych w skali CAQI musi być wizualizowana w platformie informacyjnej oraz w aplikacjach mobilnych.
8. Na ogólnodostępnej platformie oraz w aplikacjach mobilnych musi zostać zapewniony dostęp do danych historycznych z ostatnich 24 godzin (PM1, PM2.5, PM10, temperatura, wilgotność, ciśnienie).
9. Na platformie internetowej oraz w aplikacjach mobilnych mają być prezentowane prognozy zanieczyszczenia powietrza na kolejne 24 godziny ze sprawdzalnością na poziomie minimum 80%. Prognozowana wartość zanieczyszczenia powietrza ma być prezentowana w skali CAQI (forma liczbowa oraz graficzna) w odniesieniu do skali kolorystycznej stosowanej do wizualizacji wyników pomiarów. Zamawiający zapewnia sobie możliwość zweryfikowania sprawdzalności prognozy zanieczyszczeń powietrza.
10. Wykonawca zapewni możliwość generowania raportów, zawierających dane dotyczące stężeń pyłów (PM1, PM2.5, PM10) oraz dane pogodowe (temperatura, wilgotność, ciśnienie) w cenie abonamentu dostępne w wersji online w indywidualnym panelu klienta. System musi posiadać możliwość generowania wyników pomiarów w formie tabel i wykresów dla poszczególnych parametrów i określonych ram czasowych tj. raporty dobowe, tygodniowe, miesięczne, roczne.
11. Wykonawca na platformie internetowej oraz w aplikacjach mobilnych musi prezentować dane dotyczące sponsora czujnika tj. jego nazwę oraz jego logo (logotyp/herb). Ponadto Wykonawca musi zapewnić interaktywny link umożliwiający przekierowanie na wskazaną przez Zamawiającego stronę internetową (stronę internetową sponsora czujnika).
12. System monitorowania jakości powietrza musi zapewnić dostęp do API z danymi pomiarowymi.
13. Platforma musi być dostosowana dla osób niepełnosprawnych (słabowidzących, osób z dysfunkcją wzrokową).

7.8. PSZOK – licencja szt. 1 – wymagania minimalne

Wymagania funkcjonalne dla modułu obsługi ePSZOK

1. Moduł musi umożliwiać obsługę zadań związanych z ewidencją odpadów przyjmowanych w punkcie selektywnej zbiórki odpadów komunalnych (PSZOK) oraz prowadzenia szczegółowej ewidencji ilościowo jakościowej w zakresie odebranych odpadów.
2. Moduł musi być zaprojektowany w modelu trójwarstwowym:
   - warstwa danych,
   - warstwa aplikacji,
   - warstwa prezentacji.

   Powinien być obsługiwany przynajmniej przez dwie ogólnodostępne przeglądarki internetowe w aktualnych wersjach wspieranych przez producenta. Architektura systemu powinna umożliwiać pracę jedno i wielostanowiskową, zapewniać jednokrotne wprowadzanie danych tak, aby były one dostępne dla wszystkich użytkowników. System musi zapewniać weryfikację wprowadzanych danych w formularzach i kreatorach. Zapewnienie bezpieczeństwa danych zarówno na poziomie danych wrażliwych jak i komunikacji sieciowej powinno być przy zastosowaniu bezpiecznych protokołów sieciowych.
3. Moduł musi umożliwiać pracy na urządzeniach mobilnych (np. tablet) podłączonych do sieci internetowej możliwością ograniczenia połączenia do określonych adresów IP.
4. W zakresie administrowania użytkownikami moduł powinien umożliwić wprowadzenie dowolnej ilość użytkowników i zdefiniować ich role (np.: administrator systemu, operator, kierownik, gmina) z określeniem zakresu czynności wykonywanych w systemie.

5. Moduł powinien wspierać zdalny odczyt z wag elektronicznych za pośrednictwem serwisu komunikującego się z elektroniką wagową (system w swojej funkcjonalności powinien przewidywać możliwość włączenia obsługi wag przy założeniu iż będzie taka możliwość techniczna).
6. Moduł w zakresie ewidencyjnym obsługi odbioru odpadów powinien umożliwić prowadzenie:
   - ewidencji osób przekazujących odpady minimum w zakresie imię, nazwisko, oraz danych adresowych i kontaktowych w powiązaniu z ewidencją posesji z których są przyjmowane odpady,
   - ewidencji nieruchomości z których są odbierane odpady (złożone deklaracje) minimum z zakresie adresu posesji, nr działki, identyfikacji karty mieszkańca w powiązaniu z ewidencją osób przekazujących odpady
   - ewidencji przyjęć odpadów, umożliwiającą ewidencjonowania:
     - daty i godziny oddania odpadów
     - danych osoby przekazującej odpady,
     - dane nieruchomości z której pochodzą odpady,
     - nr rej. pojazdu przywożącego odpady,
     - waga całkowitej oddanych odpadów,

   szczegółowej informacji o przyjmowanych rodzajach odpadów (nazwa i rodzaj odpadu, ilość/waga, jednostka materiałowa, magazyn składowania itp.).
7. Moduł musi umożliwić definicję rodzajów odpadów w zakresie nazwy, kod rodzaju odpadu oraz określania obowiązującego dla niego limitu i jego sposobu wyliczenia.
8. W zakresie określenia limitów odpadów powinna być możliwość definicji limitów na przyjmowane rodzaje odpadów obejmująca m.in.:
   - okres obowiązywania limitu,
   - wysokość limitu (wagowa lub ilościowa),
   - określenie jednostka na którą przyznany jest limit (np. rok, kwartał, miesiąc) oraz liczba jednostek czasu w których ma być wyliczany (np. 1 rok, 1 kwartał, 4 miesiące),
   - wybór sposobu uwzględniania jednostki czasu przy ustaleniu przekroczenia limitu – wg kalendarza (np., bieżący rok, miesiąc) lub wyliczane wstecz do daty ostatniego przekazywania odpadów,
   - możliwość określenia stawki opłaty po przekroczeniu limitu.
9. Moduł powinien współpracować z systemem do ewidencji opłat za gospodarowanie odpadami funkcjonującym w gminie z możliwością automatycznej weryfikacji danych osoby przekazującej odpady poprzez specjalistyczny serwis (usługa web service) systemu gminnego na podstawie kodu kreskowego, karty mieszkańca lub numeru PESEL i informowanie operatora minimum w zakresie informacji o złożeniu deklaracji i niezaleganiu z opłatami za odpady. W celu usprawnienia wprowadzania danych system musi umożliwić po zidentyfikowaniu w systemie gminnym osoby oddającej odpady pobranie niezbędnych danych potrzebnych do wypełnienia formularza odbioru odpadów poprzez przekazanie danych przez web service systemu gminnego.
10. Moduł powinien umożliwić obsługę odpłatnego przyjęcia odpadów, z automatycznym wyliczeniem kwoty opłaty z uwzględnieniem określonych limitów i stawek obowiązujących przy ich przekroczeniu. System powinien wydrukować dokument z określeniem danych niezbędnych do uregulowania opłaty.
11. Kontrola zdefiniowanych limitów powinna być dokonywana w trakcie przyjmowania odpadów. System informuje użytkownika o fakcie przekroczenia limitu, wielkości przekroczenia oraz ewentualnej kwoty dopłaty.
12. Moduł musi umożliwić wydruk dokumentu potwierdzającego przyjęcie odpadów z uwzględnieniem danych osoby oddającej oraz informacji o odebranych ilościach odpadów.
13. W zakresie składowania odpadów (magazyny) system powinien umożliwić:
   - prowadzenie ewidencji magazynów (miejsc składowania poszczególnych odpadów)
   - prowadzenie ewidencji stanów magazynowych dla poszczególnych rodzajów odpadów z uwzględnieniem automatyczne przeliczania stanów na podstawie przyjęć i przekazań odpadów,
   - możliwość wprowadzania korekt stanów magazynowych.
14. Moduł powinien posiadać ewidencję przekazań odpadów obejmującą data przekazania, dane transportującego odpady, dane przyjmującego odpady, rodzaj odpadów, waga odpadów, metoda zagospodarowania.

15. Moduł powinien umożliwić wydruk potwierdzenia przekazania odpadów.
16. Moduł powinien zapewnić integrację z Bazą danych odpadowych minimum w zakresie:
    - importu kontrahenta z BDO,
    - importu kodów odpadów z BDO
    - wglądu w Karty Ewidencji Odpadów Komunalnych z bazy BDO,
    - utworzenia nowej Karty Ewidencji Odpadów Komunalnych w bazie BDO,
    - wygenerowania Kart Ewidencji Odpadów Komunalnych w bazie BDO na podstawie poprzedniego roku,
    - aktualizacji Kart Ewidencji Odpadów Komunalnych w bazie BDO na podstawie przyjęć odpadów
    - utworzenia Karty Przekazania Odpadu Komunalnego w bazie BDO na podstawie przekazania odpadów,
    - wglądu w Karty Przekazania Odpadów Komunalnych z bazy BDO.
17. W zakresie analizy danych system powinien umożliwiać:
    - wgląd w historię przyjęć odpadów dla klienta i nieruchomości,
    - wgląd w wykorzystanie limitów dla danej nieruchomości,
    - podsumowanie przyjęć odpadów na poszczególne rodzaje odpadów w zadanym okresie czasu,
    - podsumowanie przyjęć odpadów na poszczególne rodzaje odpadów w zadanym okresie czasu dla wybranego klienta lub nieruchomości,
    - zestawienie przyjęć odpadów (łącznie lub na wskazany rodzaj odpadu) w poszczególnych dniach w zadanym okresie czasu,
    - podsumowanie przekazań odpadów na poszczególne rodzaje odpadów w zadanym okresie czasu.
18. Moduł powinien umożliwić założenia ewidencji podmiotów odbierających odpady z uwzględnieniem ich nr rejestrowego, nazwy, adres siedziby oraz adresu miejsca prowadzenia działalności w powiązaniu z BDO.
19. System powinien umożliwić przekazywanie zwrotnej informacji o odebranych odpadach do systemu gminnego odpowiedzialnego za naliczanie opłat za gospodarowanie odpadami w powiązaniu z posesją, z której zostały one odebrane. Użytkownik system gminnego powinien mieć wgląd w ilości odebranych odpadów, daty wizyt na PSZOK z poziomu kartoteki systemu dziedzinowego. Wymiana danych powinna odbywać się za pośrednictwem metod serwisu komunikacyjnego (web service) z możliwością wywołania przez operatora w dowolnym momencie funkcji przekazania danych do urzędu za określony okres. System może też przekazywać te dane bezpośrednio po zakończeniu odbioru odpadów od klienta.

7.9. eRada – licencja szt. 1 – wymagania minimalne

1. Wszystkie poniższe funkcjonalności musza być zgodne z obowiązującymi przepisami prawa w opisanym zakresie (np. kodeksem cywilnym, kodeksem postępowania administracyjnego, ustawami i rozporządzeniami dot. stosowania podpisu elektronicznego, itd.)
2. Przygotowywanie i elektroniczna dystrybucja porządku obrad wraz z materiałami dla radnych poprzez konto użytkownika w systemie.
3. Funkcja importu porządku obrad bezpośrednio z pliku .docx, .doc (Word).
4. Możliwość dodawania dokumentów przez administratorów do wbudowanego w systemie repozytorium plików.
5. Możliwość dodawania do porządku obrad załączników w postaci elektronicznej takich jak projekty uchwał, załączniki do uchwał, mapy, prezentacje, itp. załączniki w formatach *.doc, *.docx, *.pdf, *.xls, *.xlsx, *.jpg, *.jpeg, *.bmp, *.ppt, *.pptx.
6. Możliwość eksportowania dokumentów z edytora aktów prawnych – Legislator do systemu obsługi Rady
7. Możliwość dodawania linków do punktów w utworzonym posiedzeniu.
8. Możliwość dodawania prywatnych notatek do posiedzenia przez operatora oraz radnych.
9. Możliwość edytowania porządku obrad w trakcie posiedzeń.
10. Możliwość wydrukowania materiałów sesyjnych.
11. Zarządzanie bazą kontaktów i wewnętrzną komunikacją między biurem rady, a radnymi z możliwością przesyłania wiadomości poprzez e-mail oraz SMS. Archiwizowanie przesyłanych wiadomości w systemie z możliwością sprawdzenia historii korespondencji.

12. Tworzenie głosowań jawnych (imiennych), zwyczajnych (tajnych), oraz specjalnych (np. do rzeprowadzania różnego rodzaju wyborów).
13. Możliwość tworzenia głosowań z własnymi odpowiedziami.
14. Możliwość zabezpieczenia głosowań kodem PIN ustalonym przez administratora oraz jego wyświetlenie na ekranie prezentacyjnym podczas głosowania.
15. Możliwość automatycznego i ręcznego sprawdzenia listy obecności radnych z możliwością ręcznej modyfikacji tej listy, na wypadek spóźnień czy wcześniejszych wyjść.
16. Generowanie raportu obecności z informacją o obecności radnych w poszczególnych punktach porządku obrad.
17. Sprawdzanie obecność w trakcie posiedzenia w formie głosowania.
18. Możliwość złożenia przez radnego interpelacji w formie elektronicznej.
19. Brak możliwości oddawania głosu przez osoby oznaczone jako nieobecne na posiedzeniu
20. Prezentacja wyników głosowań na urządzeniach wszystkich osób biorących udział w głosowaniach
21. Możliwość zabezpieczenia głosowania na podstawie adresu IP z którego będą przyjmowane glosy – zewnętrzny adres sieci urzędowej, w celu wyeliminowania możliwości oddania głosów przez osoby przebywające poza urzędem.
22. Dostęp do systemu za pomocą urządzeń mobilnych oraz komputerów umożliwiający:
    - sprawdzenie kalendarium posiedzeń nadchodzących oraz archiwalnych,
    - przeglądanie porządków obrad i wyników głosowań,
    - pobieranie i przeglądanie załączników,
    - głosowanie (oddawanie głosów) w czasie rzeczywistym podczas posiedzenia poprzez wybór jednego z 3 przycisków: „za”, „przeciw”, „wstrzymuję się”.
    - zgłaszanie się do dyskusji i przeglądanie listy osób planujących wypowiedź w danej sprawie w czasie rzeczywistym podczas posiedzenia.
    - funkcję wewnętrznego komunikatora dla radnych.
23. Elektroniczna i interaktywna obsługa posiedzeń poprzez:
    - elektroniczną rejestrację radnych zgłaszających się do dyskusji nad projektami uchwał i innymi materiałami będącymi przedmiotem obrad,
    - elektroniczną rejestracje wniosków formalnych,
    - elektroniczną obsługę głosowań podczas sesji (głosowania jawne imienne),
    - prezentację porządku obrad oraz dostęp do załączników w czasie posiedzenia,
    - możliwość dynamicznej modyfikacji porządku obrad oraz materiałów na posiedzenia z automatycznym odświeżaniem zmian na urządzeniach radnych,
    - prezentację przedmiotu głosowania, listy osób uprawnionych do głosowania i wyników głosowania w czasie posiedzenia,
    - dynamiczne zarządzanie listą gości, którym udziela się głosu podczas posiedzenia,
    - możliwość ustawienia czasu wypowiedzi oraz wyświetlanie w czasie posiedzenia licznika czasu wypowiedzi i komunikatu o przekroczeniu czasu wypowiedzi,
    - zatwierdzanie uchwał,
    - przygotowanie projektów protokołu z posiedzeń z automatycznym przekazywaniem wyników głosowań,
    - rejestrację dźwięku w systemie informatycznym z możliwością transkrypcji dźwięku na tekst przy wykorzystaniu zewnętrznego oprogramowania,
    - rejestrację dźwięku w systemie informatycznym wraz ze scenariuszem prezentującym punkty porządku obrad oraz wypowiadające się przy tych punktach osoby z możliwością odsłuchania konkretnej wypowiedzi po wybraniu jej ze scenariusza,
    - umożliwienie poprzez sieć Internet dostępu mieszkańcom i podmiotom zainteresowanym do transmisji z posiedzenia (na żywo), przeglądania porządku obrad wraz z załącznikami (bieżących oraz archiwalnych) oraz przeglądanie wyników głosowań.
24. Możliwość tworzenia wewnętrznego rejestru uchwał oraz jego automatyczne publikowanie dla mieszkańców i podmiotów zainteresowanych.
25. Dostęp interesantów do kalendarza radnego informującego o planowanych dyżurach.

26. Możliwość integracji z systemami zewnętrznymi Zamawiającego – Wykonawca zobowiązuje się udostępnić API umożliwiające integracje w zakresie przesyłania danych dostępnych w systemie do obsługi Rady.
27. System obsługiwany będzie przez laptopy z systemem Windows lub urządzenia mobilne z systemem android nie starszym niż wersja 4.4.
28. Automatyczna transkrypcja dźwięku nagrania sesji na tekst w ramach systemu eRada w formacie odpowiednim do tworzenia napisów do sesji.
29. Możliwość zagłosowania przez administratora w imieniu radnego.
30. Możliwość ustawienia głosowania w ten sposób, ze wybór jest jednej z dwóch lub więcej opcji/możliwości.
31. Możliwość określenia trybu głosowania na: głosowanie zwykłą większością głosów, głosowanie bezwzględną większością głosów, głosowanie bezwzględną większością głosów ustawowego składu rady, głosowanie kwalifikowaną większością.
32. Automatyczne zamknięcie i zapisanie listy głosowań po zagłosowaniu przez wszystkich radnych.
33. Możliwość zamknięcia głosowania przez administratora w sytuacji, gdy radny obecny na posiedzeniu nie bierze udziału w głosowaniu.
34. Możliwość określenia grup użytkowników oraz nadania im stosownych uprawnień;
35. Możliwość udostępniania wszystkim radnym, jak również pojedynczym adresatom, np. tylko członkom danej komisji, komunikatów, które niekoniecznie muszą dotyczyć posiedzeń czy sesji wraz z udostępnieniem dowolnych plików tzw. „Informator”.
36. Możliwość podglądu przez administratora w historię odczytu posiedzenia, jak i dołączonych dokumentów, załączników do porządku obrad, komunikatów przez poszczególnych radnych.
37. Możliwość sprawdzenia przez administratora aktywności użytkowników i ilości logowań, kiedy się one odbywały, ostatnia aktywność w systemie użytkownika, ostatnie logowanie.

System powinien być kompatybilny ze sprzętem opisanym w punkcie eRada – sprzęt komputerowy.

1. Transmisje mają być zintegrowane z systemem do obsługi Rady w zakresie Automatycznego wyświetlania w transmisji informacji o:
   1.1. aktualnie przemawiającej osobie
   1.2. aktualnie omawianym punkcie z porządku obrad
   1.3. uruchomionym głosowaniu i temacie tego głosowania
   1.4. wynikach głosowania
   1.5. o trwającej przerwie
   1.6. nazwie instytucji i dacie posiedzenia
2. System ma zapewniać możliwość automatycznego przewinięcia archiwalnego nagrania wideo do wybranego przez oglądającego punktu porządku obrad,
3. Automatyczne kadrowanie mówcy w momencie udzielenia głosu w systemie do obsługi Rady
4. Podczas okresu obowiązywania gwarancji wymagana jest transmisja oraz archiwizacja nagrań z sesji o minimalnej jakości 720p poprzez serwery Wykonawcy.
5. Integracja systemu obsługi rady z systemem konferencyjnym.
   5.1. Zgłoszenie chęci zabrania głosu:
      5.1.1. Chęć zgłoszenia do głosu przez radnego musi być możliwa z poziomu tabletu oraz pulpitu konferencyjnego
      5.1.2. Zgłoszenie z poziomu tabletu spowoduje pojawienie się radnego na liście osób chętnych do zabrania w systemie obsługi rady oraz zaświecenie wskaźnika LED na szyjce mikrofonu przypisanym do radnego w kolorze innym niż kolor aktywnego mikrofonu.
      5.1.3. Zgłoszenie z poziomu pulpitu konferencyjnego spowoduje zaświecenie wskaźnika LED na szyjce mikrofonu przypisanym do radnego w kolorze innym niż kolor aktywnego mikrofonu oraz umieszczenie radnego na liście osób chętnych do zabrania głosu w dyskusji
   5.2. Udzielenie radnemu zgody na zabranie głosu:

5.2.1. Udzielenie zgody na głos jest możliwe z poziomu aplikacji do obsługi rady dla administratora oraz poprzez aplikację na urządzeniu przewodniczącego
5.2.2. Udzielenie głosu spowoduje zmianę koloru wskaźnika LED umieszonego na szyjce mikrofonu na kolor inny niż w przypadku chęci zabrania głosu oraz aktywuje mikrofon
5.3. Wykonawca dostarczy zamawiającemu aplikację do integracji wraz z danymi uwierzytelniającymi, którą zamawiający będzie mógł samodzielnie zainstalować na dowolnym urządzeniu z systemem Windows
6. Wymagania dodatkowe:
6.1. Publikacja materiałów sesyjnych oraz wyników przeprowadzonych głosowań w Internecie w oparciu o infrastrukturę techniczną Wykonawcy.
6.2. Przechowywanie danych na serwerach znajdujących się na terytorium Rzeczypospolitej Polskiej.
6.3. Udostępnienie kopii zapasowej oprogramowania oraz danych wprowadzonych przez Zamawiającego na żądanie Zamawiającego.
7. Montaż oraz parametryzacja wszystkich urządzeń po stronie Wykonawcy w siedzibie Zamawiającego.

7.10. E-Rada sprzęt komputerowy – 1 kpl. – wymagania minimalne

System transmisji z obrad (2 kamery, komputer do transmisji, monitor, montaż po stronie Wykonawcy)

1. Kamera do transmisji IP – 2 sztuki
1.1. Praca w standardzie TCP/IP,
1.2. przetwornik 1/2.8” STARVIS,
1.3. obiektyw w zakresie 5-80 mm,
1.4. zoom optyczny 16x,
1.5. protokoły sieciowe: IPv4, SSL, RTSP, DHCP, UPnP,
1.6. zasilenie PoE
1.7. ONVIF.
2. Centrala system konferencyjnego – 1 szt.
2.1. Jednostka sterująca systemu konferencyjnego.
2.1.1. Funkcjonalność i parametry techniczne:
2.1.1.1. Kontrola otwartych mikrofonów pozwalająca wybrać minimum 4 otwarte mikrofony
2.1.1.2. Wbudowany rejestrator dźwięku może nagrywać dyskusję w formacie MP3 do pamięci wewnętrznej lub pamięci USB
2.1.1.3. Napięcie zasilania sieciowego od 100 do 240 VAC ± 10%
2.1.1.4. Maks. od 1,6 A (100 VAC) do 0,7 A (240 VAC)
2.1.1.5. Liczba pulpitów dyskusyjnych na jednostkę sterującą minimum 40
2.1.1.6. Minimalna częstotliwość próbkowania 44,1 kHz
2.1.1.7. Maksymalna waga 3.4 kg
2.1.1.8. Materiał metal lakierowany
2.1.1.9. Metoda montażu stołowy lub w szafie typu Rack 19”
2.1.1.10. Wymiary maksymalne (wys. X szer. X gł.) 45 x 483 x 300
2.1.1.11. Temperatura pracy od 5 do 45°C
2.1.1.12. Złącza umieszczone na obudowie:
2.1.1.12.1. Z przodu jednostki:
2.1.1.12.1.1. Minimum 1 x złącze USB
2.1.1.13. Z tyłu jednostki:
2.1.1.13.1. Minimum 1 x wyjście analogowe
2.1.1.13.2. Minimum 1 x wejście analogowe
2.1.1.13.3. Minimum 1 x złącze Ethernet RJ45 do komunikacji
2.1.1.14. Kontrola dyskusji odbywa się poprzez wybór jednego z dostępnych trybów dyskusji:
2.1.1.14.1. Tryb otwarty - uczestnicy mogą mówić, naciskając przycisk na swoim mikrofonie. Gdy maksymalna liczba otwartych mikrofonów zostanie

osiągnięta, następny uczestnik, który naciśnie przycisk swojego mikrofonu, zostanie dodany do listy oczekujących. Pierwszy uczestnik z listy oczekujących będzie mógł mówić, gdy zostanie wyłączony któryś z aktywnych mikrofonów

2.1.1.14.2. Tryb z wyciszaniem - uczestnicy mogą wyciszać się wzajemnie przez włączanie swojego mikrofonu. Gdy maksymalna liczba otwartych mikrofonów zostanie osiągnięta, następny uczestnik, który naciśnie przycisk na swoim mikrofonie, zdezaktywuje mikrofon, który był najdłużej aktywny (mikrofon, który posiada przewodniczący nie jest uwzględniany w liczbie otwartych mikrofonów i dlatego nie może go wyciszyć żaden inny uczestnik).

2.1.1.14.3. Tryb aktywacji głosowej - uczestnicy mogą aktywować swoje mikrofony, mówiąc do nich. Mikrofon może być czasowo wyciszony poprzez naciśnięcie i przytrzymanie przycisku mikrofonu.

3. Mikrofon konferencyjny/Jednostki konferencyjne (pulpity dyskusyjne) – 24 sztuk, funkcjonalność i parametry techniczne:
   - 3.1. Szyjka mikrofonu o długości minimum 480 mm oraz minimum jednym przegubie.
   - 3.2. Przycisk aktywacji mikrofonu musi umożliwiać uczestnikowi włączanie/wyłączanie mikrofonu lub (w zależności od trybu aktywacji mikrofonu) zgłoszenie chęci wypowiedzi. Wokół, nad lub od spodu przycisku musi znajdować się podświetlany wskaźnik LED informujący o aktywnym mikrofonie (preferowany kolor czerwony).
   - 3.3. Wbudowane 3,5 mm stereofoniczne gniazdo słuchawkowe
   - 3.4. Odporność na zakłócenia z sieci GSM
   - 3.5. Sygnalizacja świetlna umieszczona na szyjce mikrofonowej wskazująca włączenie i żądanie zabrania głosu (np. pierścień lub wskaźniki LED w dwóch kolorach – preferowany zielony oraz czerwony)
   - 3.6. Szeregowa topologia połączeń, każdy z pulpitów musi posiadać gniazdo przelotowe.
   - 3.7. Wbudowany wysokiej jakości głośnik
   - 3.8. Możliwość konfiguracji dowolnego pulpitu jako jednostki przewodniczącego lub dostarczenie pulpitu dedykowanego dla przewodniczącego.
   - 3.9. Pasmo przenoszenia urządzenia obejmuje zakres częstotliwości od 200 Hz do 12,5 kHz
   - 3.10. Impedancja obciążenia słuchawek > 8 Ω < 1 k Ω
   - 3.11. Maksymalne wymiary urządzenia bez mikrofonu (wys. X szer. X gł.) 65 x 210 x 150 mm
   - 3.12. Ciężar ok. 1 kg
   - 3.13. Montaż stołowy
   - 3.14. Materiał plastik, metal
   - 3.15. Temperatura pracy od 0 do 35°C

7.11. Wodomierze z nakładka radiową – szt. 1379 – wymagania minimalne

1. Wymagania ogólne

Modernizacja sieci wodociągowej poprzez wymianę wodomierzy na wodomierze z odczytem radiowym wraz z wdrożeniem systemu „e-woda”.

Do prawidłowego działania systemu Zamawiający wymaga dostawy Zestawów pomiarowo-komunikacyjnych. Zestaw pomiarowo-komunikacyjny to urządzenie, które w czasie rzeczywistym rejestruje i zapisuje dane o zużyciu, alarmach pojawiających się u odbiorcy oraz różnego typu anomaliach.

Podstawą zestawu jest moduł radiowy umieszczony na liczniku **(nie dotyczy ultradźwięków),** który rejestruje dane z licznika, za pomocą zaprogramowanych algorytmów analizuje je i wysyła informacje drogą radiową. W chwili zbliżenia się z odbiornikiem radiowym do czujników bezprzewodowo zebrane zostaną dane od kontrahentów. W tym samym czasie odbiornik danych radiowych przekazuje je za pomocą bluetooth do urządzenia, gdzie są one wizualizowane. Moduł pracować ma w paśmie radiowym o częstotliwości 868 MHz, w sposób jednokierunkowy (spełniając wymagania Rozporządzenia Ministra Administracji I Cyfryzacji z dnia 12 grudnia 2014 roku w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia radiowego (t.j. Dz. U. z 2017 r. poz. 96)). Transmisja ma umożliwiać nieprzerwaną pracę modułu co najmniej 10 lat.

Zastosowany system transmisji danych musi eliminować wady rozwiązań optycznych i kontaktronowych, przekaz ten ma być odporny na zanieczyszczenia, pyły i wilgoć.

Licznik - ostatnią częścią zestawu pomiarowo-komunikacyjnego jest licznik, którego zakres pomiarowy nie może być niższy niż R≥160-H, w zakresie średnic DN 15-20. Transfer danych do modułu elektronicznego musi się opierać na indukcyjnej (Ti) metodzie skanowania licznika ze wskazówki licznika **(nie dotyczy ultradźwięków)**.

2. Wodomierze

Przedmiotem zamówienia jest:
a) Dostawa wraz z montażem wodomierzy jednostrumieniowych suchobieżnych wraz ze skonfigurowanymi modułami radiowymi do zdalnego odczytu w ilości 1 286 sztuk:
DN15 R≥160-H, Q3=2,5 L110 – 148 szt.,
DN20 R≥160-H, Q3=4,0 L130 – 1 120 szt.,
DN20 R≥160-H, Q3=4,0 L130 - 18 szt. – z wyniesioną anteną pasywną.
b) Dostawa wraz z montażem wodomierzy ultradźwiękowych wraz ze skonfigurowanymi modułami radiowymi do zdalnego odczytu w ilości 93 sztuk:
DN 25 R250 L160 Q3=6,3 – 8 szt.,
DN 25 R250 L260 Q3=6,3 – 35 szt.,
DN 32 R250 L260 Q3=10,0 – 30 szt.,
DN 40 R250 L300 Q3=16,0 – 20 szt.,
c) Dostawa 3 szt. kompletów urządzeń do zdalnego odczytu i konfiguracji modułów radiowych wraz z anteną samochodową do montażu na dachu samochodu,
d) Dostawa oprogramowania jako licencji lub usługi (SaaS) do odczytu, przechowywania oraz przetwarzania danych, pochodzących z radiowego odczytu liczników na urządzenia mobilne i stacjonarne na okres 10 lat kompatybilnego z oprogramowaniem firmy PZI TARAN Sp. z o.o. (Mielec) stosowanym aktualnie w tutejszym Przedsiębiorstwie w ramach zarządzania i realizacji zadań w zakresie gospodarki wodno-ściekowej oraz rozliczeń.

Wymagania techniczne dotyczące wodomierzy DN15 – 20: R≥160

1. Wodomierze fabrycznie nowe ze znakiem oceny zgodności zgodnym z rokiem produkcji oraz dostawy.
2. Zgodne z Rozporządzeniem Ministra Gospodarki z dnia 23.10.2007 w sprawie wymagań, którym powinny odpowiadać wodomierze, oraz szczegółowego zakresu sprawdzeń wykonywanych podczas prawnej kontroli metrologicznej tych przyrządów pomiarowych (Dz. U. z 2007 r. nr 209, poz. 1513).
3. Aktualny atest higieniczny PZH
4. Zgodne z Dyrektywą Parlamentu Europejskiego i Rady 2014/32/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku przyrządów pomiarowych (wersja przekształcona).
5. Podlegające ocenie zgodności, posiadające certyfikat badania typu WE i deklarację zgodności producenta z Dyrektywą 2014/32/UE Urządzeń Pomiarowych MID oraz normą EN14154 lub równoważną w języku polskim lub przetłumaczonej na język polski.
6. Korpus wodomierza wykonany z mosiądzu.
7. Temperatura pracy: do 30˚C.
8. Ciśnienie robocze: do 16 bar.
9. Liczydło wodomierza hermetyczne klasy IP68, obrotowe, z dokładnością odczytu 1 litr, ośmiobębenkowe.
10. Odporność wodomierza na zewnętrzne pole magnetyczne (czteropolowe sprzęgło magnetyczne, pierścień antymagnetyczny (nie dotyczy wodomierzy ultradźwiękowych)).
11. Dwustronne łożyskowanie wirnika na kamieniach technicznych,
12. Możliwość montażu bezpośrednio na liczydle wodomierza modułu radiowego (bez użycia adapterów), w trakcie eksploatacji, bez uszkodzenia znaku oceny zgodności, wyklucza się rozwiązania oparte na nadajnikach kontaktronowych i optycznych.
13. Możliwość aktualnego odczytu wzrokowego stanu wodomierza w przypadku uszkodzenia lub awarii nakładki radiowej.

14. Możliwość rozbudowania o dodatkowe/zamienne urządzenie w przypadku ciężkich warunków odczytu (głębokie, zalane wodą studnie).

Wymagania techniczne dotyczące wodomierzy ultradźwiękowych DN25-40 R≥250:
1. Wodomierze fabrycznie nowe z cechą legalizacyjną w roku dostawy.
2. Aktualny atest higieniczny PZH.
3. Zgodne z Dyrektywą Parlamentu Europejskiego i Rady 2014/32/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku przyrządów pomiarowych (wersja przekształcona).
4. Podlegające ocenie zgodności, posiadające certyfikat badania typu WE i deklarację zgodności producenta z Dyrektywą 2014/32/UE Urządzeń Pomiarowych MID oraz normą EN14154 lub równoważną w języku polskim lub przetłumaczonej na język polski.
5. Korpus wodomierza wykonany z metalu, nie dopuszcza się korpusów wykonanych z kompozytu.
6. Odporność wodomierza na działanie zewnętrznych pól magnetycznych.
7. Niski próg rozruchu.
8. Wodomierz posiadający 480 rejestrów dziennych, 36 rejestrów miesięcznych, 16 rejestrów rocznych.
9. Liczydło wodomierza hermetyczne klasy IP68.
10. Ciśnienie robocze do 16bar.
11. Maksymalna temperatura pracy do 50ºC.
12. Brak konieczności stosowania odcinków prostych przed i za wodomierzem
13. Alarm pustej rury, anormalnej temperatury.
14. Zasilanie bateryjne, żywotność baterii min. 10 lat, bateria jonowa wymienna.
15. Możliwość montażu modułu radiowego, w trakcie eksploatacji, bez uszkodzenia cech legalizacyjnych.
16. Możliwość aktualnego odczytu wzrokowego stanu wodomierza w przypadku uszkodzenia lub awarii modułu komunikacyjnego.

Wymagania techniczne dotyczące modułów radiowych:
1. Konstrukcja modułowa (oddzielna od wodomierza). Nie dopuszcza się rozwiązań zintegrowanych w liczydle wodomierza oraz zespolonych z wodomierzem w sposób trwały, które w przypadku demontażu modułu naruszałyby cechy legalizacyjne wodomierza lub powodowały konieczność demontażu całego wodomierza z instalacji, a także za pomocą adapterów.
2. Montaż modułu bezpośrednio na liczydle wodomierza.
3. Częstotliwość nośna w wolnym od opłat paśmie radiowym.
4. Nie dopuszcza się rozwiązań opartych na nadajnikach kontaktronowych i optycznych.
5. Wymagana klasa szczelności modułu: IP68 w tym modułów z wyniesioną anteną.
6. Zasilanie modułu: bateria litowa o żywotności powyżej 10 lat. Dla systemów jednokierunkowych żywotność ta musi być zachowana przy ustawieniu wysyłki danych minimum co 15s.

Funkcje modułu radiowego:
7. Podanie aktualnego wskazania wodomierza w momencie odczytu,
8. Podanie informacji o alarmach, w tym:
8.1. przy użyciu magnesu neodymowego,
8.2. demontażu modułu radiowego,
8.3. przecieku z podaniem ilości dni w miesiącu,
8.4. stanie baterii,
8.5. przepływie wstecznym,
9. Aktualna data i godzina odczytu (z uwzględnieniem czasu letniego i zimowego oraz lat przestępnych),
10. Podanie informacji o przepływach wstecznych,
11. Rejestr wskazań licznika z poprzednich 12 miesięcy (wskazanie, przepływ wsteczny)
12. Historia alarmów z 12 miesięcy
13. Funkcje programowalne modułu:
13.1. Aktualna data i godzina,
13.2. Aktualne wskazanie wodomierza,

13.3. W przypadku transmisji jednokierunkowej: interwał czasowy pomiędzy kolejnymi transmisjami radiowymi, programowalne miesiące, dni, godziny w których moduł radiowy dokonuje transmisji danych,
13.4. Próg alarmu przepływu wstecznego,
13.5. Próg alarmu wycieku

Wymagania techniczne dotyczące montażu

1. Wykonawca wykona kompleksową usługę demontażu „starych" wodomierzy (w ilości 1379 szt.) z przyłączy wodociągowych potwierdzonych protokołem. Zdemontowane wodomierze Wykonawca przekaże Zamawiającemu. Zamawiający zapewni przestrzeń magazynową do przechowywania zdemontowanych i nowych wodomierzy na czas realizacji zamówienia.
2. Wykonawca zamontuje wodomierz ze skonfigurowanym modułem na węzłach urządzeń rejestrujących oraz po montażu zestawów pomiarowych oplombuje węzły urządzeń rejestrujących plombą z tworzywa sztucznego, z numerem seryjnym i kodem kreskowym montowaną na śrubunek na przyłączach wodociągowych wskazanych przez Zamawiającego.
3. Montaż ma się odbywać przy pomocy aplikacji dla Zamawiającego lub wskazanych przez niego podmiotów do wymiany wodomierzy. Postęp prac ma być widoczny dla Zamawiającego w trybie online. Wykonawca na czas realizacji zamówienia zainstaluje u Zamawiającego lub wskaże adres strony internetowej, na której po zalogowaniu będzie mógł nadzorować postęp prac w zakresie:
3.1. Weryfikacji danych w trakcie prowadzonych wymian;
3.2. Ilości podjętych prób montażu pod danym adresem;
3.3. Rejestrowania daty i godziny wykonania danej wymiany/serwisu;
3.4. Rejestrowania w czasie rzeczywistym aktualnego status zlecenia;
3.5. Nadzorowanie ilości i jakości zdarzeń, pozwoli na ewentualną natychmiastową reakcję ze strony Zamawiającego;
3.6. Rejestrowania materiałów wykorzystanych przy wymianie wodomierza;
3.7. Wygenerowania protokołu z wymiany urządzenia rejestrującego z możliwością zapisu w formie pliku .pdf
3.8. Dostępu do zdjęć z wykonanych prac, zdemontowanego liczydła wodomierza, nowo zamontowanego wodomierza (szczegółowe wymagania dotyczące zakresu zdjęć są opisane poniżej).
3.9. Raportowania efektywności prac, poziomu wykonania.
3.10. Generowania zestawień w formacie Excel;
3.11. Eksportu protokołów w formie zbiorczego pliku.
4. Wzór elektronicznego protokołu wymiany wodomierza Wykonawca uzgodni przed przystąpieniem do wykonania usługi.
5. Aplikacja, ma umożliwiać skanowanie kodów kreskowych i kodów QR znajdujących się na urządzeniach rejestrujących, modułach radiowych i plombach.
6. Jeśli Wykonawca po zakończonej wymianie wodomierza w danym punkcie pomiarowym podejmie się prac serwisowych w szczególności, w przypadku konieczności usunięcia wad stwierdzonych w trakcie odbioru musi stworzyć następny protokół wykonanych prac. Protokół ten nie może zastępować protokołu wymiany. Zamawiający sprawdzając postęp prac pod danym adresem ma mieć dostęp do obu dokumentów.
7. Wykonawca, za pomocą aplikacji, zobowiązuje się wykonać 4 czytelne zdjęcia cyfrowe:
   - Pierwsze zdjęcie umożliwiające odczytanie numeru seryjnego i stanu demontowanego urządzenia rejestrującego,
   - Drugie zdjęcie umożliwiające odczytanie numeru seryjnego wodomierza, modułu i stanu nowego wodomierza,
   - Trzecie zdjęcie numeru montowanej plomby,
   - Czwarte zdjęcie po montażu na węźle wodomierzowym wodomierza z modułem z widocznym plombowaniem węzła wodomierzowego,
   - W/w zdjęcia powinny być wykonane i/lub opisane w taki sposób aby w ich nazwie zawarta była lokalizacja (adres) oraz na zdjęciu data i godzina jego wykonania.
8. Zamawiający zakłada, iż dla części lokalizacji prace montażowe mogą wymagać dodatkowej ingerencji poza wymianą samego wodomierza. Wszelkie prace dodatkowe niewchodzące w zakres

wymiany samego wodomierza będą realizowane na podstawie ewentualnego dodatkowego zlecenia Zamawiającego.

9. W przypadku konieczności ich wymiany Zamawiający zapewni niezbędne śrubunki mosiężne do zamontowania wodomierza. Wykonawca odbierze śrubunki mosiężne w siedzibie Zamawiającego, po wcześniejszym uzgodnieniu ich ilości i terminu odbioru.
10. Wykonawca dostarczy cennik prac dodatkowych (nie stanowiących zakres zamówienia jakim jest dostawa i montaż wodomierzy jak np. mrożenie sieci, wykonanie przeróbki, usunięcie awarii, wymiana zaworu), z którego Zamawiający będzie mógł skorzystać w chwili wystąpienia potrzeby. Dostarczenie cennika prac dodatkowych pozwoli na rozliczenie prac dodatkowych zgodnie z faktycznie wykonanymi pracami i zużytym materiałem.
11. W przypadku konieczności usunięcia awarii na przyłączu wodociągowym, która uniemożliwia montaż wodomierza (m.in. niesprawna nawiertka, niesprawny zawór główny przed urządzeniem pomiarowym) Wykonawca poinformuje o zaistniałej sytuacji Zamawiającego, a ten dokona niezbędnych napraw własnymi siłami i środkami.
12. O usunięciu w/w awarii Zamawiający poinformuje Wykonawcę, niezwłocznie po jej wystąpieniu, maksymalnie do tygodnia czasu od momentu jej powstania.
13. Zamawiający zezwala Wykonawcy na zlecenie w/w czynności osobom trzecim pod warunkiem prowadzenia przez Wykonawcę nadzoru nad pracami wykonywanymi przez osoby trzecie oraz przy zachowaniu pełnej odpowiedzialności Wykonawcy za prawidłowe i terminowe wykonanie usługi.
14. Wykonawca zobowiązany jest do przeprowadzenia dwóch prób montażu. Jeżeli z przyczyn niezależnych od Wykonawcy nie będzie możliwości realizacji prac (np. brak dostępu do urządzeń) w pierwszym podanym terminie, Wykonawca musi wyznaczyć drugi, zastępczy termin ich wykonania. Za drugim razem zamawiający zobowiązany jest do ustalenia terminu wymiany urządzenia. Brak możliwości wykonania prac musi być udokumentowany fotograficznie z zaznaczeniem daty i miejsca wykonania zdjęcia. W razie dwukrotnego podjęcia próby montażu zakończonej niepowodzeniem ze względu na nieobecność odbiorcy lub brak dostępu do wodomierza, przyjmuje się, że usługa została wykonana zgodnie z warunkami umowy, a odpowiedzialność za dokonanie rzeczywistego montażu urządzenia spoczywa na Zamawiającym. Strony mogą odrębnie ustalić dodatkowe terminy montażu w przypadkach opisanych w niniejszym punkcie, pod warunkiem pokrycia przez Zamawiającego ich kosztów wg cennika Wykonawcy.

Urządzenia do odczytu i konfiguracji modułów

1. Wykonawca ma obowiązek dostawy trzech kompletów urządzeń do odczytu i konfiguracji modułów radiowych w tym m.in. odbiornika radiowego z możliwością podłączenia dodatkowej anteny samochodowej; urządzenia do konfiguracji i odczytu zaprogramowanych parametrów modułu radiowego oraz urządzenia mobilnego (smartphone/tablet) do wizualizacji odczytanych danych.
2. Urządzenie mobilne (tablet/smartfon) z kolorowym wyświetlaczem o przekątnej co najmniej 6”, działający w oparciu o jeden z najpopularniejszych systemów operacyjnych (co najmniej android lub iOS) o podwyższonej odporności potwierdzonej certyfikatem MIL-STD-810H, wodoodporny i pyłoszczelny min. IP68 zgodnie z normą IEC 60529 lub równoważną, posiadający min. 24 miesięczną gwarancję producenta. Kompatybilny z dostarczonym systemem zdalnego odczytu, skanerem radiowym, anteną, głowicą. Jeżeli w celu zachowania kompatybilności konieczne jest dostarczenie dodatkowego oprogramowania/licencji, obowiązek ten spoczywa na Wykonawcy.
3. Dostawa licencji lub oprogramowania jako usługi (SaaS) do odczytu, przechowywania oraz przetwarzania danych, pochodzących z radiowego odczytu liczników na urządzenia mobilne i stacjonarne na okres 10 lat.

Wymagania dotyczące oprogramowania:

1. Oprogramowanie przechowujące dane na serwerze zewnętrznym w tzw. „chmurze”. Zamawiający nie posiada wolnej przestrzeni serwerowej. Dopuszcza się rozwiązania serwerowe jeśli Wykonawca zapewni dostawę serwerów w ramach dostawy systemu wraz z niezbędnym oprogramowaniem i licencjami oraz zapewni jego konserwację i amortyzację przez 10 lat od daty podpisania umowy.
2. Oprogramowanie w języku polskim,
3. Możliwość importu plików w formacie minimum .csv,
4. Możliwość eksportu plików w formacie .csv; .xml; .txt,

5. Możliwość kreowania wzoru eksportu plików,
6. Możliwość współpracy z systemem rozliczeniowo – księgowym Zamawiającego PZI TARAN - GOSKOM Premium w układzie wymiany plików,
7. Archiwizacja pomiarów z okresu 10 lat.
8. Wykonawca bądź bezpośredni producent oferowanych urządzeń podpisze z Zamawiającym umowę powierzenia przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa a w szczególności zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) („RODO").
9. Dane zebrane z modułów radiowych za pomocą zestawu odczytowego mają trafić do oprogramowania jako licencji lub usługi (SaaS) dalej oprogramowania, w którym użytkownicy systemu mogą tworzyć trasy odczytowe, analizować zebrane dane i generować raporty do wystawienia faktur. Oprogramowanie ma spełniać następujące funkcje:
    1. Możliwość tworzenia dowolnej ilości kont użytkowników. Każdy użytkownik posiadający indywidualny login i hasło.
    2. Możliwość przydzielania uprawnień użytkownikom z podziałem uprawnień dla poszczególnych grup (np. inkasent, fakturowanie, administrator)
    3. Możliwość zawieszania bądź aktywowania danego konta przez Administratora.
    4. Masowe importowanie i walidacja wprowadzanych danych (zabezpieczenie użytkownika przed dwukrotną próbą wpisania tego samego nr wodomierza lub modułu).
    5. Możliwość zarządzania licznikami bezpośrednio w przeglądarce internetowej z każdego miejsca z dostępem do Internetu,
    6. Nielimitowana możliwość dodawania i usuwania wodomierzy i modułów.
    7. Przegląd i analiza odczytów. W jednym oknie platformy dostęp do wszystkich odczytów z jednej trasy – aktualnych wskazań, zaistniałych alarmów, ich lokalizacji na mapie.
    8. Możliwość wstawienia komentarza dotyczącego poszczególnego odbiorcy zarówno przez osobę odczytującą jak i administratora danych.
    9. Szczegółowe informacje dotyczące kontrahenta. Dostęp do historii odczytów, zdarzeń zarejestrowanych na danym wodomierzu z modułem radiowym.
    10. Zarządzanie trasami. Platforma powinna dopuszczać tworzenie dowolnej ilości tras, dodawanie nowych instalacji do już stworzonej trasy, aktywowanie lub dezaktywowanie danej trasy, edycję trasy, wizualizowanie trasy na mapie, przypisywanie konkretnych tras danemu inkasentowi.
    11. Generowanie raportów. Platforma powinna zapewniać proste i intuicyjne tworzenie raportów za pomocą szablonów, np. do integracji z systemem rozliczeniowo-bilingowym.
10. Wykonawca zapewni dostęp do serwisu online i aplikacji oraz wsparcie techniczne wolne od opłat w ciągu min. 10 lat od zakupu ostatniej partii wodomierzy z modułami radiowymi.
11. Wykonawca zapewni aktualizacje oprogramowania do najnowszej wersji niezbędnej do prawidłowego funkcjonowania oprogramowania i aplikacji na urządzenie mobilne w okresie 10 lat od zakupu ostatniej partii wodomierzy z modułami.
12. Wykonawca zapewni dostęp do oprogramowania za pomocą strony internetowej wolnej od opłat, w tym opłat hostingowych w ciągu 10 lat od zakupu ostatniej partii wodomierzy z modułami.
13. Oprogramowanie musi umożliwiać odczytywanie i wizualizację wszystkich danych zbieranych przez moduły radiowe opisane SWZ. W tym m.in. wykresy w oparciu o zużycie wody, przepływ wsteczny.
14. Oprogramowanie musi umożliwiać identyfikację wodomierzy z skonfigurowanymi modułami, nazw odbiorców, adresów zainstalowania urządzeń rejestrujących (tzw. punktów poboru), aktualnego stanu liczydła urządzenia rejestrującego i informacji o wielkości zużytej wody w okresach miesięcznych.
15. Oprogramowanie musi umożliwiać automatyczne nanoszenie lokalizacji modułów radiowych na mapie elektronicznej oraz korektę lokalizacji w przypadku, gdy automatyczna lokalizacja dla danego adresu byłaby niemożliwa lub niedokładna.
16. Oprogramowanie musi umożliwiać dowolną konfigurację wyszukiwania i filtrowania danych np. po numerze urządzenia rejestrującego, numerze modułu radiowego, adresie punktu poboru i/lub po nazwie odbiorcy usług.

17. Oprogramowania na tablet/smartphone i komputer mają być ze sobą ściśle zintegrowane i synchronizowane.
18. Aplikacja na tablet/smartphone ma być intuicyjna i ergonomiczna, by nie powodowała wśród obecnych pracowników uczucia wykluczenia społecznego ze względu na nowe technologie, a tym samym dawała możliwość pracy na niej osobom starszym i niepełnosprawnym. Wymagania te Wykonawca spełni poprzez:
    1. minimalizm w zakresie wyboru opcji zadań do wykonania (do 10 opcji wyboru na poszczególnych widokach);
    2. aplikacja w języku polskim;
    3. widok modułów radiowych do odczytania w formie mapy (wolnej od opłat dla Zamawiającego) i listy do wyboru przez użytkownika;
    4. możliwość weryfikacji postępu odczytu danej trasy za pomocą intuicyjnej wizualizacji np. moduły nie odczytane kolor żółty, moduły odczytane kolor zielony, moduły z alarmem kolor czerwony.
    5. możliwość wejścia na wybrany moduł po kliknięciu na dany adres;
    6. możliwość odczytania w chwili odczytu anomalii: alarm wycieku, przepływu wstecznego, przyłożenia magnesu, demontażu modułu, niskiego stanu baterii;
19. Aplikacja musi być zabezpieczona indywidualnym loginem i hasłem użytkownika.
20. Zarządzanie hasłami (nadawanie uprawnień, zmiana hasła, tworzenie nowych użytkowników) ma być możliwe wyłącznie z poziomu Oprogramowania.
21. Aplikacja musi mieć możliwość pracy offline ze względu na możliwy brak zasięgu LTE/3G.
22. Aplikacja mobilna musi posiadać opcję szybkiego i prostego wyboru trasy, którą w danej chwili chcemy odczytać.
23. Po połączeniu z dostępnym Wi-Fi aplikacja powinna dawać możliwość bezprzewodowej synchronizacji tras, które zostały przygotowane w Oprogramowaniu.
24. Po połączeniu z dostępnym Wi-Fi aplikacja powinna dawać możliwość bezprzewodowej wysyłki odczytanych danych do Oprogramowania.
25. Dane możliwe do zaprogramowania w modułach radiowych z poziomu aplikacji:
    1. zmiana daty i godziny,
    2. zmiana/wybór trybu wysyłania (w jakich godzinach w jakich dniach)
    3. zmiana/wybór danych, które powinny być wysyłane z urządzenia
    4. zmiana progów alarmowych w tym: alarmu wycieku oraz wstecznego przepływu,
    5. zmiana stanu licznika,
    6. możliwość usunięcia wcześniejszych alarmów,
    7. możliwość wyczyszczenia całej pamięci modułu,
    8. dostęp do historii wskazań z ostatnich 12 miesięcy,
    9. dostęp informacji na temat urządzenia.

Szczegółowe ilości wodomierzy

Dostawa i montaż wodomierza jednostrumieniowego DN 15 o parametrach: Q3 = min 2,5 m3/h, GZ 3/4, długość 110 mm, R≥160 -H, , korpus mosiężny z kompletem uszczelek i plombą numeryczną z modułem podstawowym.	148
Dostawa i montaż wodomierza jednostrumieniowego DN 20 o parametrach: Q3 = min 4,0 m3/h, GZ 1, długość 130 mm, R≥160 -H, korpus mosiężny z kompletem uszczelek i plombą numeryczną z modułem podstawowym.	1120
Dostawa i montaż wodomierza jednostrumieniowego DN 20 o parametrach: Q3 = min 4,0 m3/h, GZ 1, długość 130 mm, R≥160 -H, korpus mosiężny z kompletem uszczelek i plombą numeryczną z modułem wyniesionym na przewodzie – antena pasywna	18
Dostawa i montaż wodomierza ultradźwiękowego DN25 o parametrach: Q3= 6,3 m3/h, GZ 1 ¼, długość 160 mm, R≥250 w każdej pozycji montażu, korpus mosiężny z kompletem uszczelek i plombą numeryczną z modułem wyniesionym na przewodzie.	8
Dostawa i montaż wodomierza ultradźwiękowego DN25 o parametrach: Q3= 6,3 m3/h, GZ 1 ¼, długość 260 mm, R≥250 w każdej pozycji montażu, korpus mosiężny	35

z kompletem uszczelek i plombą numeryczną z modułem wyniesionym na przewodzie.	
Dostawa i montaż wodomierza ultradźwiękowego DN32 o parametrach: Q3= 10 m3/h, GZ 1 ½, długość 260 mm, R≥250 w każdej pozycji montażu, korpus mosiężny z kompletem uszczelek i plombą 30 numeryczną z modułem wyniesionym na przewodzie.	30
Dostawa i montaż wodomierza ultradźwiękowego DN40 o parametrach: Q3= 16 m3/h, GZ 2, długość 300 mm, R≥250 w każdej pozycji montażu, korpus mosiężny z kompletem uszczelek i plombą numeryczną z modułem wyniesionym na przewodzie.	20
Wodomierze i moduły powinny posiadać karty katalogowe. Minimalny wymagany okres gwarancji urządzeń pomiarowych - 36 miesięcy od daty dostarczenia. Konstrukcja wodomierzy DN20 suchobieżna, (całkowicie sucha przekładnia oraz liczydło).	nd

7.12. System eWoda – licencja szt. 1 – wymagania minimalne

Zamawiający informuje, że posiada obecnie system TARAN. Wymaga rozbudowy i aktualizacji tego systemu lub dostawy nowego rozwiązania o poniższych funkcjonalnościach:

1. System musi posiadać wspólną z systemem finansowo-księgowym kartotekę płatników-odbiorców zawierającą minimum: dane adresowe, dane bankowe, rodzaje odbiorców, dane dotyczące zawartych umów z klientem.

2. Kartoteka płatników-odbiorców musi umożliwiać jej wydruk oraz filtrowanie według: (numeru umowy)kodu odbiorcy, nazwiska, adresu, nazwy (ogólne pole), adresu posesji (punktu odbioru mediów) oraz obsługiwać filtrowanie i sortowanie wg wybranego pola z listy.

3. System musi posiadać kartotekę zawierającą minimum: numer punktu odbioru, numer książki z liczbą porządkową, numer (identyfikator) inkasenta, adres punktu, opis punktu, dane niezbędne do naliczenia opłaty za dostawę wody i odbiór ścieków zarówno w odniesieniu do opłat ustalanych na podstawie odczytów wodomierzy jak i opłat ryczałtowych oraz opłat stałych w powiązaniu z wybraną taryfą, dane dotyczące wodomierzy z uwzględnieniem czy jest to wodomierz główny czy podlicznik.

4. W zakresie odczytów radiowych system powinien ewidencjonować dane z układów pomiarowych umożliwiające automatyzację procesu zdalnego odczytu bez konieczności ręcznego przyporządkowania odczytów do poszczególnych układów pomiarowych.

5. System powinien umożliwiać eksport danych ewidencjonowanych układów pomiarowych w formacie zgodnym z oferowanym systemem do zdalnego odczytu.

6. Po wykonaniu importu danych z systemu zdalnego odczytu powinna być możliwość automatycznego naliczenia opłat dla grupy odbiorców, których układy pomiarowe zostały odczytane. Operator systemu powinien mieć możliwość wyselekcjonowania odbiorców dla których nie zostały wykonane odczyty.

7. System musi posiadać kartotekę liczników zawierającą: kod dodatkowy licznika, numer fabryczny licznika, numer układu pomiarowego dla zdalnych odczytów, średnica, typ licznika, ile cyfr licznika, data zabudowy licznika, data legalizacji licznika, numer plomby licznika, numer wskaźnika licznika, historię wskazań (odczytów), zużycie licznika z wymiany, średnia wartość zużycia.

8. System musi umożliwiać operacje na punktach: wymiana wodomierza, wymiana spowodowana legalizacją lub uszkodzeniem, naliczanie średniego zużycia, zapamiętywanie

odczytu starego wodomierza (doliczanie do faktury), przegląd wymian wodomierzy, przeniesienie punktu na inny, renumeracja pozycji w książce.

9. System musi umożliwiać rejestrację odczytów umożliwiając: pokazywanie danych wprowadzanego punktu/odbiorcy, zbiorcze wprowadzanie odczytów dla punktów odbiorcy, całej książki, doliczanie zużycia z wymiany, obliczanie średniego zużycia w przypadku uszkodzenia licznika, obliczanie bieżącego zużycia, pokazywanie informacji o relacjach: punkt nadrzędny/podlicznik, przegląd odczytów dla bieżącego punktu, przegląd i drukowanie odczytów dla odbiorcy, informowanie użytkownika o odchyleniach od średniego zużycia (np. powyżej 30%).

10. System musi umożliwiać wystawianie faktur, w szczególności musi uwzględniać: wystawianie faktur dla pojedynczego odbiorcy, wpisywanie daty wystawienia i płatności, spisywanie uwag do faktury, możliwość modyfikacji wzoru wydruku faktury (logo, rozmieszczenie), uwzględnianie na fakturze: zaległości odbiorcy, nadpłaty odbiorcy, należnych odsetek za wpłaty po terminie, kosztów upomnienia, drukowanie kodów kreskowych, zatwierdzenie bądź anulowanie faktury, wystawianie zbiorcze faktur: dla książki, przeglądanie wystawionych faktur, zestawienie wystawionych faktur, wystawianie raportu dla banków dotyczących wystawionych faktur, tworzenie raportu poleceń zapłaty.

11. System powinien zapewnić tworzenie i wydruk rejestrów sprzedaży wraz z zapisem jego do formatu (struktury) JPK_VAT, JPK_V7M oraz JPK_V7K.

12. System musi umożliwiać rozliczenie odbiorcy dla faktur od podanej daty wystawienia oraz za zadany przez użytkownika okres.

13. System powinien umożliwiać automatyczną wysyłkę wystawionych faktur na wskazany adres email.

14. Moduł powinien umożliwiać przygotowywanie raportu TransGUS do GUS-u.

15. System powinien umożliwiać wysyłanie komunikatów SMS oraz e-mail do odbiorców zarówno indywidualnie jak i do wybranej grupy odbiorców. Powinna być możliwość selekcji odbiorców na podstawie miejscowości, trasy, określonej grupy odbiorców, dat dokonania odczytu lub braku odczytu w zadanym okresie, wystawienia faktury w danym okresie. Operator systemu może następnie wprowadzić treść komunikatu i przesłać ją do wybranej grupy.

7.13. Integracja (Platforma e-usług publicznych) – 400 rbh – wymagania minimalne

Pełna integracja oferowanych rozwiązań z platformą EBOM (krajowy węzeł identyfikacji elektronicznej, obieg dokumentów EZD, system dziedzinowy urzędu, eBOM , formularze ePUAP, e-Doręczenie, mObywatel (ePłatności PeP) – minimum 200 godzin.
Szacowany podział godziny:

- eBOM - elektroniczne Biuro Obsługi Mieszkańca - 40 godz.
- Oprogramowanie dziedzinowe - 80 godz.
- Planowanie budżetu - 30 godz.
- System GIS - 30 godz.
- e-edukacja - 40 godz.
- Obieg dokumentów - 30 godz.
- Monitoring środowiska - 20 godz.
- PSZOK - 15 godz.
- eRada - 20 godz.
- System eWoda - 20 godz.
- Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa - 20 godz.
- Oprogramowanie do zarzadzania infrastrukturą IT - 20 godz.
- Oprogramowanie do wirtualizacji - 20 godz.
- e-Rada sprzęt komputerowy - 15 godz.

W ramach prac związanych z integracją oferowanych systemów Wykonawca zobowiązany jest do zapewnienia wymiany danych pomiędzy systemami oferowanymi w ramach postepowania jak i oferowaną platformą do realizacji e-Usług (platforma eBOM) oraz wykorzystywanymi systemami zewnętrznymi i platformami centralnymi uczestniczącymi przy realizacji e-Usług. Zakres prac obejmie dostawę w/w serwisów oraz ich niezbędną modyfikację celem uzyskania spójnej platformy e-Usługowej z zapewnioną bezpieczną wymianą danych oraz standardem zgodnym z wymogami prawa oraz stosowanymi praktykami. Oferowane rozwiązania jeżeli wymagają stosowania odpowiednich certyfikatów oraz przejścia procedur odbiorowych powinny zostać dostarczone kompletne wraz z wymaganym testem akceptacyjnym (np. integracja z Krajowym Węzłem Identyfikacji Elektronicznej, system płatności elektronicznych, mObywatel itp.). Minimalny zakres prac (usług) szacowany jest na 320 roboczogodzin. Integracja obejmie w swoim zakresie następujące systemy (platformy):

- Centralną platformę e-Usług (eBOM) dostarczaną w ramach projektu
- Krajowy Węzeł Identyfikacji Elektronicznej
- System dziedzinowy urzędu w zakresie niezbędnym dla wymagań eBOM i systemu EZD
- System Elektronicznego Zarządzania Dokumentami (EZD - obieg dokumentów)
- System do realizacji zdalnych odczytów wodomierzy
    - Import odczytów z zewnętrznych systemów odczytujących (nakładki radiowe) przez wystawione REST API.
    - Analizy kompletności i poprawności odczytów.
    - Generowania faktur na podstawie zaimportowanych odczytów.
    - Zapisania faktur sprzedaży w formacie pdf i wysyłka ich e-mailem (e-faktury).
    - Przechowywanie obrazu oryginału oraz kopii faktur sprzedaży w formie elektronicznej.
- Platformę ePUAP (zarówno w zakresie pobierania danych z formularzy jak i samej wysyłki o odbierania dokumentów za pośrednictwem systemu EZD)
- System e-Doręczeń - w zakresie umożliwiającym emitowanie, odbieranie i wysyłanie korespondencji bezpośrednio w Systemie, bez potrzeby korzystania z portalu
- Krajowy System e-Faktur (KSeF) – w zakresie określonym ustawą,
- Serwis **GUS** – w celu weryfikowania poprawności danych kontrahentów
- **ZUS Płatnik** – w zakresie wymaganym przepisami
- **ZUS PUE** – w zakresie obsługi zwolnień lekarskich
- **Biała Lista** www.podatki.gov.pl w celu weryfikowania poprawności podanych numerów kont bankowych

Z uwagi na to, że system Elektronicznego Zarządzania Dokumentami (EZD) oraz portal eBOM będą stanowił rdzeń integracyjny wszystkich systemów dziedzinowych oraz e-Usług wdrażanych w ramach projektu, funkcjonalność modułu integracyjnego musi być zrealizowana w oparciu o jego interfejsy komunikacyjne.

Minimalne wymagania funkcjonalne:

- Moduł musi posiadać ustandaryzowane interfejsy zewnętrzne, obejmujące udostępnianie usług integracyjnych (m.in. wymiany danych), systemom zewnętrznym poprzez: usługi Web Services (w oparciu o standardy SOAP 1.2, WSDL co najmniej 1.1); możliwość komunikacji z wykorzystaniem plików XML zlokalizowanych w strukturach plikowych jednostki, JMS, zgodność ze standardami XML 1.0 i XSD 1.1.
- Komunikacja z systemem EZD odbywać się ma za pośrednictwem serwisu komunikacyjnego.
- Moduł musi zapewniać integrację modułów dziedzinowych systemów informatycznych z systemem Elektronicznego Zarządzania Dokumentami. Musi być możliwość automatycznego przekazywania dokumentów tworzonych w tych modułach wraz z automatycznym dodawaniem ich do teczek spraw bezpośrednio w systemie EZD.
- Moduł musi zapewniać integrację systemu EZD z systemem finansowo-księgowym. Musi być możliwość przekazywania do systemu FK danych w zakresie niezbędnych do jego zaksięgowania wynikających z wpływających dokumentów finansowych na dziennik podawczy (np. faktury, umowy itp.).
- Moduł musi pozwalać na integrację z systemem kadrowo-płacowymi na poziomie obsługi wniosków urlopowych, czasu pracy.
- Moduł musi zapewniać synchronizację kartotek kontrahentów na poziomie modułów dziedzinowych i systemu EZD zapewniając dwukierunkową wymianę metadanych dokumentów

przysyłanych z platformy ePUAP oraz systemu e-Doręczeń lub funkcjonować w oparciu o wspólne zasoby bazodanowe.

- Moduł musi zapewniać automatyzację następujących procesów:
  - Faktury przychodzące rejestrowane w systemie EZD muszą być kierowane bezpośrednio do modułu FK zapewniając jednokrotne wprowadzanie danych.
  - Umowy rejestrowane w systemie EZD kierowane są bezpośrednio do modułu Rejestr Umów zapewniając jednokrotne wprowadzanie danych.
  - Dokumenty elektroniczne dotyczące wszystkich typów deklaracji podatkowych (wypełnionych na ePUAP lub w systemie e-Doręczeń) muszą być przekazywane poprzez EZD do modułów podatkowych zapewniając pobierania metadanych z plików XML w systemie dziedzinowym.
  - Dokumenty elektroniczne dotyczące deklaracji za gospodarowania odpadami komunalnymi (wypełnionych na ePUAP), muszą być przekazywane poprzez EZD do modułów podatkowych zapewniając czytywanie metadanych z plików XML w dedykowanym module dziedzinowym.
  - Dokumenty elektroniczne dotyczące oświadczeń o sprzedaży napojów alkoholowych (wypełnionych na ePUAP) muszą być przekazywane poprzez EZD do modułu związanego z obsługą zezwoleń na sprzedaż napojów alkoholowych zapewniając pobierania metadanych z plików XML w systemie dziedzinowym.
  - Decyzje elektroniczne pochodzące z modułów podatkowych muszą być przekazywane do systemu EZD (obsługa podpisu elektronicznego jest realizowana z poziomu EZD), a następnie kierowane na skrytkę ePUAP podatnika lub na konto w systemie e-Doręczeń.
  - Niezbędną wymianę danych z platformą ePłatności (mObywatel - PeP)
- Moduł musi umożliwić udostępnianie do publikację dokumentów (rejestrów) na stronie podmiotowej BIP oraz musi umożliwić informowanie o statusie sprawy na stronie podmiotowej BIP.
- Moduł musi umożliwiać publikowanie dokumentów wraz z danymi teczek spraw celem ich wizualizacji na platformie eBOM.
- Moduł musi udostępniać metody komunikacyjne niezbędne do funkcjonowania portalu eBOM w zakresie udostępnienia odpowiednich danych zapewniając ich wizualizację po stronie www, możliwość dokonania zapłaty za pośrednictwem systemu płatności elektronicznych oraz dostarczania odpowiednich komunikatów do interesantów.
- Moduł musi posiadać mechanizm kontroli dostępu do usług pozwalający na dostęp do danej usługi ze względu na użytkownika oraz grupę (jednostkę organizacyjną) do której należy.
- Moduł musi umożliwiać administratorom zarządzanie udostępnianymi usługami i interfejsami (w tym harmonogramem komunikacji, lokalizacją plików, uprawnieniami do nich). Moduł będzie umożliwiał wdrażanie nowych interfejsów komunikacyjnych.

7.14. Instalacja i konfiguracja (Platforma e-usług publicznych) – 200 rbh – wymagania minimalne

Prace wdrożeniowe obejmują niezbędny zakres prac związanych z instalacją i konfiguracją systemu oraz wprowadzeniem niezbędnych parametrów pracy systemu celem prawidłowego udostępniania e-usług oraz pracy operatorów systemu. Instalacja systemu z wyjątkiem portali e-usług musi być przeprowadzona na infrastrukturze serwerowej Zamawiającego. Do obowiązków wykonawcy będzie odpowiednia konfiguracja urządzeń sieciowych oraz zapewnienie bezpieczeństwa przetwarzania danych. Prace konfiguracyjno-instalacyjne nie mogą zakłócić bieżącej pracy urzędu (zapewnienie ciągłości działania systemów). Prace te będą też obejmowały niezbędna modyfikację oferowanych systemów celem ich integracji z platformą sprzętowa Zamawiającego. Do obowiązków Wykonawcy należeć będzie także odpowiednia konfiguracja serwisów hostowanych na zewnątrz w zakresie wymiany danych z systemem dziedzinowym funkcjonującym na infrastrukturze Zamawiającego. Wszelkie niezbędne certyfikaty i zabezpieczenia (także te wymagane przez integrowane systemy centralne) muszą być dostarczone przez Wykonawcę i nie mogą wymagać dodatkowych opłat. Jeżeli konfiguracja systemu będzie wymagała zmian w ustawieniach serwera bazy albo strukturze serwerowej Zamawiającego wszelkie prace muszą zostać wykonane przez Wykonawcę i nie mogą wymagać dodatkowych kosztów, jeżeli wymagane będzie dostarczenie dodatkowego oprogramowania to koszty te zarówno związane z jego zakupem jak i późniejszym utrzymaniem w okresie trwałości projektu ponosi Wykonawca.
Szacowany podział godzinowy:

- eBOM - elektroniczne Biuro Obsługi Mieszkańca - 20 godz.
- Oprogramowanie dziedzinowe - 40 godz.
- Planowanie budżetu - 30 godz.
- System GIS - 25 godz.
- e-edukacja - 20 godz.
- Obieg dokumentów - 15 godz.
- Monitoring środowiska - 15 godz.
- PSZOK - 15 godz.
- eRada - 10 godz.
- System eWoda - 10 godz.

7.15. Digitalizacja zasobów – 100 rbh – wymagania minimalne

Digitalizacja zasobów GIS z obszaru zabytków (karta zabytków) – 950 szt.:

1. Digitalizacja obejmuje wprowadzenie do cyfrowego rejestru zabytków gminnych, informacji przekazanych przez zamawiającego w formie zgłoszeń, wydruków map, tabeli, zestawień, projektów zagospodarowania terenów (PZT), szkiców sytuacyjnych dla istniejących obiektów,
2. Utworzenie rejestru zabytków w formie tabelarycznej i powiązanie każdego obiektu z lokalizacją przestrzenną w oparciu o EGIB, GESUT, PZT/szkic sytuacyjny lub wizję terenową,
3. Utworzenie rozszerzenia zawartości i funkcji w obrębie istniejącej aplikacji użytkowanej w urzędzie. Rozszerzenie powinno obejmować:
   a) Zarządzanie bazą danych zabytków na terenie gminy,
   b) Dodawanie obiektów punktowych poprzez zlokalizowanie obiektów w przestrzeni,
   c) Wprowadzenie obiektu w bazie danych przestrzennych poprzez ujawnienie pełnych informacji dotyczących: zabytków,
   d) Automatyzację ewidencji zabytków poprzez powiązanie zgłoszenia z geometrią działek ewidencyjnych i wyświetlanie informacji o zgłoszeniach na mapie oraz w tabeli atrybutów,
   e) Dla rejestru tabelarycznego zabytków powinien obejmować atrybuty w zakresie minimum: numeru sprawy, dacie złożenia zgłoszenia, danych wnioskodawcy, numeru działki lub działek ewidencyjnych, na których jest zlokalizowany obiekt, adresie działki lub działek ewidencyjnych, dacie budowy obiektu. Szczegółowy zakres atrybutów zostanie uzgodniony z wykonawcą na etapie realizacji projektu,
   f) Dla rejestru tabelarycznego zabytków powinien obejmować atrybuty. Szczegółowy zakres atrybutów zostanie uzgodniony z wykonawcą na etapie realizacji projektu,
   g) Możliwość dodania innych informacji do bazy danych istotnych dla prowadzenia sprawy w urzędzie. Szczegółowy zakres atrybutów zostanie uzgodniony z wykonawcą na etapie realizacji projektu,
   h) Prezentacja obiektów rejestru w widoku mapy z zastosowaną odpowiednią stylizacją (klasyfikację obiektu) z etykietą, w odniesieniu do działek ewidencyjnych,
   i) Korzystanie z opcji auto podpowiedzi przy wpisywaniu numerów działek ewidencyjnych tak, aby zapewnić wyszukiwanie z podaniem jedynie części szukanego ciągu znaków,
   j) Korzystanie z opcji auto uzupełniania danych o adresie firmie świadczącej usługę wywozu nieczystości poprzez pobieranie danych ze słownika z możliwością jego edycji.
   k) Przypisywanie załączników do konkretnych obiektów poprzez nazwanie załącznika i wskazanie lokalizacji pliku na dysku użytkownika. Można dodać załączniki w dowolnym formacie i liczbie,
   l) Dostęp do załączników danego obiektu z poziomu rejestru lub z widoku mapy.
   m) wprowadzenie danych wnioskodawcy (możliwość wyboru z bazy lub dodanie nowego): dane personalne (imię, nazwisko lub nazwa, NIP, numer KRS, REGON) i dane adresowe (miejscowość, ulica, nr budynku, nr lokalu, kod pocztowy, poczta, telefon, email),
   n) Edycję i usuwanie wprowadzanych danych z poziomu widoku mapy lub tabeli,
   o) Przeszukiwanie danych z ewidencji zbiorników bezodpływowych oraz przydomowych oczyszczalni ścieków, poprzez wpisanie fragmentu dowolnej wartości zapisanej w rejestrze,
   p) Przybliżanie okna mapy do wskazanego w tabeli rejestru obiektu,
   q) Identyfikowanie obiektów na mapie poprzez ich wskazanie,

r) Edytowanie obiektu z poziomu tabeli,
s) Zapis wybranego rejestru do pliku xlsx, csv, shp, gml,
t) Tworzenie raportów, generowanie kart informacyjnych dla obiektu z możliwością zapisu ich do pliku na dysku,
u) Generowanie sprawozdania dotyczącego gospodarowania zabytkami
v) Generowanie załączników graficznych w oparciu o przygotowane kompozycje, dostosowanie wyglądu załącznika graficznego w postaci wyboru koloru poprzez wybór koloru z palety lub poprzez wpisanie wartości RGB, szerokości i odsunięcia obrysu działki oraz wyboru dostępnych warstw w projekcie, które będą widoczne na załączniku graficznym, dostosowywanie przeźroczystości oraz etykietowania obiektów,
w) Wyświetlanie treści rejestru w połączeniu z danymi dostępnymi w bazie danych przestrzennych w gminie np.: rejestr MPZP oraz danymi dostępnymi za pomocą usług sieciowych WMS i WFS m.in. dane GDOŚ dot. ochrony środowiska, ortofotomapa, BDOT10k,
x) Wyświetlanie treści rejestru na mapie z podkładem tematycznym m.in. z portali mapowych takich jak Open Street Map, Google Maps,

4. Obsługiwanie i uruchomienie wersjonowania obiektów w rejestrach z możliwością wyświetlania danych w określonych przedziałach czasowych,
5. Uruchomienie aplikacji mobilnej dla urzędnika/pracownika urzędu pozwalającej na edytowanie atrybutów w terenie z poziomu urządzenia mobilnego opartego na systemach Android lub iOS,
6. Uruchomienie aplikacji webowej prezentującej elementy rejestru na urządzeniach mobilnych z możliwością identyfikacji obiektów na mapie z poziomu urządzenia mobilnego opartego na systemach Android lub iOS,
7. Udostępnianie danych poprzez uruchomione usługi WMS i WFS (w zakresie formatów gml i geojson), lub formatu plikowego shp, gml z możliwością dodania do istniejącego systemu informacji przestrzennej.

7.16. Szkolenia TiK Typ II – 168 rbh – wymagania minimalne

Ogólne wymogi prowadzenia szkoleń

1. Łączny czas szkoleń nie może być mniejszy 168 godzin
2. Szkolenia będą się odbywać w siedzibie Zamawiającego
3. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
4. Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
5. Szkolenia będą odbywać się w dni robocze w godzinach 7.30 – 15.30.
6. Szkolenia będą prowadzone w języku polskim.
7. Szkolenia prowadzone będą na podstawie zaakceptowanego prze Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 7 dni przed rozpoczęciem szkolenia.
8. Szkolenia prowadzone będą na podstawie zaakceptowanego prze Zamawiającego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
9. W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę kawową, trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy kawowe, trwające 15 minut każda.
10. W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.
11. W ramach organizacji szkoleń Wykonawca zapewni:
    a. Materiały szkoleniowe, obejmujące zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury bądź inne materiały dydaktyczne w formie elektronicznej lub papierowej), zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność, Wykonawca przekaże materiały szkoleniowe także Zamawiającemu w celach archiwalnych.
    b. Wystarczającą liczbę własnych licencji na oprogramowanie komputerowe wykorzystywane przy realizacji szkoleń oraz sprzęt komputerowy dla każdego Uczestnika umożliwiający przeprowadzenie szkolenia.

c. Projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń.
d. Właściwe działania informacyjne dotyczące szkoleń, w tym właściwe oznakowanie sal szkoleniowych, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych.
e. Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
f. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
   - Listy obecności Uczestników szkolenia (dzienne, wypełniane oddzielnie każdego dnia szkolenia) wraz potwierdzeniem na liście obecności przez Uczestników odbycia tego szkolenia.
   - Sporządzony przez kadrę trenerską dziennik zajęć, zawierający informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

Zakres merytoryczny szkoleń

Wykonawca w ramach zamówienia przeprowadzi szkolenia niezbędne do poprawnego uruchomienia całości modernizowanego oprogramowania oraz świadczenia e-Usług. Szkolenia obejmą minimum 80 pracowników Zamawiającego w zakresie ich obowiązków związanych z obsługa wdrażanego systemu. Szkolenia będą prowadzone w blokach tematycznych i obejmą pracowników odpowiedzialnych za realizację poszczególnych zadań. W przypadku gdy dany blok tematyczny obejmuje miększą ilość pracowników dopuszcza się szkolenia w grupach wykładowych do 15 osób oraz w grupach laboratoryjnych (praca indywidualna na komputerze) w grupach do 7 osób

Planowany minimalny zakres tematyczny szkoleń

Zakres Szkolenia, Planowana liczba uczestników szkoleń oraz godzin szkolenia.

1. Szkolenie z zakresu nowych funkcjonalności warunkujących realizację e-usług publicznych zmodernizowanego systemu dziedzinowego zintegrowanego z EZD (podział na grupy w zależności od merytoryki systemów dziedzinowych)
2. Szkolenie z zakresu Elektroniczny Obieg Dokumentów (EZD).
3. Szkolenie z obsługi Elektronicznego Biura Obsługi Mieszkańca oraz uruchamianych e-usług.
4. Szkolenie kadry kierowniczej oraz administratorów z zakresu realizacji e-usług publicznych.

Szczegółowy zakres szkoleń oraz lista osób nim objętych zostanie ustalony na etapie wdrażania systemu. Zamawiający dopuszcza zmianę ilości godzin w poszczególnych tematach szkoleń pod warunkiem realizacji łącznie minimum 168 godzin szkoleń oraz dostosowania zakresu szkoleń do celów realizacji projektu wdrożenia e-usług.

W trakcie przygotowania i przeprowadzenia szkoleń, a także przygotowania dokumentacji szkoleniowej Wykonawca zobowiązany jest przestrzegać wymagań standardu szkoleniowego i cyfrowego opisanych w dokumencie „Wytyczne dotyczące realizacji zasad równościowych w funduszach unijnych w latach 2021-2027" w brzmieniu obowiązującym na dzień podpisania umowy z wykonawcą. Tekst wytycznych dostępny jest pod adresem https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/fundusze-na-lata-2021-2027/prawo-i-dokumenty/wytyczne/wytyczne-dotyczace-realizacji-zasad-rownosciowych-w-ramach-funduszy-unijnych-na-lata-2021-2027/