Załącznik nr 1 do SWZ

Opis Przedmiotu Zamówienia

Oprogramowanie oraz infrastruktura sprzętowa

Spis treści

WSTĘP 3

I. WYMAGANIA OGÓLNE 4

1. RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ 4

II. CZĘŚĆ NR 1 6

1. UTM UNIFIED THREAT MANAGEMENT TYP 1 6
2. UTM UNIFIED THREAT MANAGEMENT TYP 2 13

III. CZĘŚĆ NR 2 21

1. SERWER 21
2. MACIERZ DYSKOWA TYP 1 33
3. MACIERZ DYSKOWA TYP 2 ..... 40~~39~~
4. UPS 47
5. ZARZĄDZALNE URZĄDZENIA SIECIOWE Z OBSŁUGĄ VLAN, MACSEC, STANDARDU 802.1X - TYP 1 49
6. ZARZĄDZALNE URZĄDZENIA SIECIOWE Z OBSŁUGĄ VLAN, MACSEC, STANDARDU 802.1X - TYP 2 51
7. ZARZĄDZALNE URZĄDZENIA SIECIOWE Z OBSŁUGĄ VLAN, MACSEC, STANDARDU 802.1X - TYP 3 53
8. OPROGRAMOWANIE ANTYWIRUSOWE ..... 55~~54~~
9. OPROGRAMOWANIE DO WYKONYWANIA KOPII ZAPASOWYCH 59

IV. CZĘŚĆ NR 3 68

1. OPROGRAMOWANIE SIEM SECURITY INFORMATION AND EVENT MANAGEMENT 68

V. CZĘŚĆ NR 4 ..... 71~~70~~

1. OPROGRAMOWANIE MOBILE DEVICE MANAGEMENT ..... 71~~70~~

VI. CZĘŚĆ NR 5 ..... 81~~80~~

1. OPROGRAMOWANIE DO MONITOROWANIA INFRASTRUKTURY INFORMATYCZNEJ ..... 81~~80~~

VII. CZĘŚĆ NR 6 82

1. URUCHOMIENIE I ŚWIADCZENIE USŁUGI SAAS W POSTACI STRONY WWW ZGODNEJ Z PRZEPISAMI PRAWA, UMIESZCZONEJ W BEZPIECZNEJ CHMURZE OBLICZENIOWEJ CHRONIONEJ ROZWIĄZANIEM ANTY-DDOS, Z ZAPEWNIENIEM KOPII ZAPASOWEJ DANYCH, AKTUALIZACJĄ SYSTEMU I ZABEZPIECZEŃ, CERTYFIKATEM SSL, WSPARCIEM TECHNICZNYM I MONITORINGIEM BEZPIECZEŃSTWA 82

WSTĘP

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Gminy Pępowo realizowanego w ramach „Cyberbezpieczny Samorząd" dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego.

I. WYMAGANIA OGÓLNE

1. RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ

1) w zakresie Oprogramowania

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności są nie gorsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane, przy czym wartość użytkowa nie może być gorsza od minimum określonego w dokumentach zamówienia. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Zamawiającego. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, zapewnić gwarancję i serwis, uwzględnić niezbędną asystę ze strony pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Mając na uwadze powyższe, w przypadku jeżeli Wykonawcy nie mają możliwości uzyskania odpowiedniego do realizacji dostępu do oprogramowania firm trzecich, w celu zapewnienia zasady konkurencyjności, przejrzystości, jawności a także równego traktowania wykonawców w trakcie prowadzenia postępowania, Zamawiający dopuszcza każdorazowo wymianę Oprogramowania u Zamawiającego pod warunkiem, że:

a) Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego systemy Wykonawca dostarcza i wdraża na swój koszt, z zachowaniem warunków licencjonowania wskazanych w niniejszym dokumencie.

b) Wykonawca przeprowadzi migrację danych w zakresie wskazanym przez Zamawiającego na swój koszt, w sposób opisany w niniejszym OPZ a migracja musi objąć pełny zakres danych bieżących i archiwalnych.

c) Wykonawca przeprowadzi instruktaże stanowiskowe, zapewni gwarancje i serwis gwarancyjny a także help desk oraz będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom Zamawiającego płynną obsługę Oprogramowania.

d) Wymiana Oprogramowania nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy wynikającą z obowiązujących terminów, przepisów prawa i stosowanych procedur.

e) Wszelkie uzgodnienia i konsultacje w zakresie transmisji danych powinny być dokonane w siedzibie Zamawiającego na podstawie zatwierdzonego harmonogramu.

f) Proces migracji musi objąć pełne dane zawarte we wcześniej użytkowanym systemie.

g) Nowe rozwiązania muszą realizować wszystkie wymienione wymagania względem Oprogramowania.

2) w zakresie Infrastruktury sprzętowej

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne".

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne".
Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w OPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne, np. zapis: "Zainstalowane min. dwa procesory 8-rdzeniowe, min. 2.8GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 127 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów." należy rozumieć jako:
"Zainstalowane co najmniej dwa procesory, posiadające co najmniej 8 rdzeni, klasy co najmniej x86, posiadające taktowanie co najmniej 2.8GHz, umożliwiające osiągnięcie wyniku co najmniej 127 w teście SPACrate2017_int_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej".

II. CZĘŚĆ NR 1

1. UTM UNIFIED THREAT MANAGEMENT TYP 1

Nazwa	Minimalne wymagania dla sprzętu
Typ	UTM Unified Threat Management typ 1 dla Urzędu Gminy w Pępowie
Wymagania Ogólne	Zamawiający posiada Fortigate 50E o nr seryjnymFGT50E5619004357 aktywnym wsparciem producenta do 2025-01-11. Zamawiający wymaga wymiany posiadanego urządzenia na model Fortigate 60F oraz wznowienia wsparcia producenta w postaci licencji min. Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) na okres do 30-06-2026. Zamawiający dopuszcza dostarczenie rozwiązania równoważnego (wymianę w/w oprogramowania wraz ze sprzętem) spełniającego poniższe wymagania minimalne. Ponadto, w przypadku dostawy oprogramowania równoważnego Zamawiający wymaga dodatkowo: • Wdrożenia • skonfigurowania • przeszkolenia administratorów z dostarczonego rozwiązania, wg ustaleń z Zamawiającym.
OPIS RÓWNOWAŻNOŚCI	
Wymagania Ogólne	System bezpieczeństwa musi realizować 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 7 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 musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów:10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 256 nie mniej niż 6.5 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 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do

	dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. • Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. • Rozwiązanie musi posiadać 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.
Połączenia VPN	1. System musi umożliwiać 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 musi posiadać 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 musi zapewniać 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 musi umożliwiać 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 musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System musi umożliwiać 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 musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System musi dysponować 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 musi współpracować 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 musi zapewniać 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 musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać 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 musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System musi mieć 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 musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać 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 musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać 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) w oparciu o zewnętrzne bazy danych. 2. System musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System musi umożliwiać 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 muszą realizować 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 musi zapewniać 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	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. Dostęp do testów wydajnościowych i funkcjonalnych oraz dokumentacji producenta należy wskazać w formularzu ofertowym.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów minimum na okres do 30.06.2026 r. Logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów ważne do 30.06.2026 r.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Ilość	1 szt.

2. UTM UNIFIED THREAT MANAGEMENT TYP 2

Nazwa	Minimalne wymagania dla sprzętu
Typ	UTM Unified Threat Management typ 2dla Gminnego Ośrodka Pomocy Społecznej w Pępowie
Wymagania ogólne	System bezpieczeństwa musi realizować 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 musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Musi istnieć możliwość dedykowania co najmniej 7 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 2. IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 4. Monitoring stanu realizowanych połączeń VPN. 5. 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 musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: • 5 portów Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 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 1 Gbps.

	6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps
Funkcje systemu bezpieczeństwa	W ramach systemu ochrony muszą być 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 musi posiadać 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 musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System mus realizować 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 musi istnieć 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 musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

	6. Polityka firewall musi umożliwiać ustawienie przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
Połączenia VPN	1. System musi 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 musi posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie kliencie VPN jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie musi zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. • Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.

	• ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. • BFD (Bidirectional Forwarding Detection). • Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcję SD-WAN	1. System musi umożliwiać 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 musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System musi umożliwiać 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 musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System musi dysponować 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 musi współpracować 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 musi zapewniać 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 musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać 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 musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być 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 musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

	2. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać 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 musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System musi pozwalać 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) 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 muszą realizować 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 musi zapewniać 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	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. Dostęp do testów wydajnościowych i funkcjonalnych oraz dokumentacji producenta należy wskazać w formularzu ofertowym.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów minimum na okres do 30.06.2026 r. Logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów ważne do 30.06.2026 r.
Gwarancja oraz wsparcie	System musi być objęty wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym

	Dniu od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora na okres do minimum 30.06.2026 r. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 . Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. Oferent winien przedłożyć dokumenty do oferty: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 lub równoważny podmiotu serwisującego.
Ilość	1 szt.

III. CZĘŚĆ NR 2

1. SERWER

Nazwa	Minimalne wymagania dla sprzętu
Typ	Sprzęt serwerowy wraz z niezbędnym oprogramowaniem dla JP - Gminnego Ośrodka Pomocy Społecznej w Pępowie
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Płyta główna musi być zaprojektowana przez producenta serwera • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane min. dwa procesory 8-rdzeniowe, min. 2.8GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 127 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
RAM	Min. 64GB DDR4 RDIMM 3200MT/s,
Funkcjonalność pamięci RAM	• Advanced ECC, • Memory Page Retire, • Fault Resilient Memory, • Memory Self-Healing lub PPR, • Partial Cache Line Sparing
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający o Min. 8GB nieulotnej pamięci cache,

	o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. o Wsparcie dla dysków samoszyfrujących
Dyski twarde	• Zainstalowane: o Min 2x dysk SSD SATA MU o pojemności min. 1.92 TB, Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. • Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
Gniazda PCI	Min. Dwa sloty PCIe LP
Interfejsy sieciowe/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet BaseT oraz min. 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Wbudowane porty	• Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, • Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 1100W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy: • możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, • możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, • możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, • 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,

	• wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
	• wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
	• automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),
	• wbudowane wsparcie instalacji i pracy na wolumenach, które:
	  • pozwalają na zmianę rozmiaru w czasie pracy systemu,
	  • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	  • umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	  • umożliwiają zdefiniowanie list kontroli dostępu (ACL),
	• wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
	• wbudowane szyfrowanie dysków
	• możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,
	• możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,
	• wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,
	• graficzny interfejs użytkownika,
	• zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
	• wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
	• możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
	• dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
	• możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	  • podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	  • 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 SSO 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, • zdalna dystrybucja oprogramowania na stacje robocze, • praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, • V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: a. dystrybucję certyfikatów poprzez http, b. konsolidację CA dla wielu lasów domeny, c. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, • szyfrowanie plików i folderów, • szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), • możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, • serwis udostępniania stron WWW, • wsparcie dla protokołu IP w wersji 6 (IPv6), • wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 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 model), • możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,

	• wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), • możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, • mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, • możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. • System serwerowy z z licencjami dostępowymi dla 8 urządzeń(hostów) łączących się z serwerem.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155 lub równoważnymi. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
	  ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
	  ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
	  ○ szyfrowane SSL
	  ○ wsparcie dla IPv6;
	  ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
	  ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
	  ○ integracja z Active Directory;
	  ○ wsparcie dla dynamic DNS;

	○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera ○ możliwość obsługi przez sześciu użytkowników jednocześnie; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o Grupowanie urządzeń w oparciu o kryteria użytkownika o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach o Szybki podgląd stanu środowiska o Podsumowanie stanu dla każdego urządzenia o Szczegółowy status urządzenia/elementu/komponentu o Generowanie alertów przy zmianie stanu urządzenia. o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń o Integracja z service desk producenta dostarczonej platformy sprzętowej

	o Możliwość przejęcia zdalnego pulpitu o Możliwość podmontowania wirtualnego napędu o Kreator umożliwiający dostosowanie akcji dla wybranych alertów o Możliwość importu plików MIB o Przesyłanie alertów „as-is" do innych konsol firm trzecich o Możliwość definiowania ról administratorów o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
Oprogramowanie do zarządzania / monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Zarządzanie: o zintegrowany kontroler zdalnego (kontroler z wbudowanym procesorem, pamięcią, kartą graficzną oraz kartę sieciową) - umożliwiający wykonywanie najpowszechniejszych zadań administracyjnych takich jak wdrożenie, konfiguracja czy aktualizacja oprogramowania układowego serwera. Dostęp

	przez przeglądarkę internetową. Licencja umożliwiająca pełne zarządzanie serwerem w tym również instalację/zatrzymywanie/uruchamianie fizycznego systemu operacyjnego (OS) - bez konieczności fizycznego dostępu do serwera • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum:

	▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o:

	▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

	• Certyfikaty
	  ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami:
	  ▪ ISO 27001 lub równoważnym
	  ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization lub równoważnym
	  ▪ CSA Cloud Control Matrix lub równoważnym

Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważnymi • Serwer musi posiadać deklaracja CE. lub równoważnym • Serwer musi spełniać wymagania normy NIST SP 800-193 lub równoważnym ochrony przed cyberatakami. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Gwarancja ON-SITE (serwis gwarancyjny wykonywany w siedzibie klienta bez dodatkowych opłat) • Zamawiający wymaga zapewnienia gwarancji Producenta na okres min. 36 miesięcy. • dostosowana do okresu gwarancji usługa zachowania dysków twardych pozwalająca na zatrzymanie uszkodzonych nośników w przypadku ich awarii oraz zutylizowanie ich zgodnie z wewnętrznymi procedurami organizacji. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany

	Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga dołączenia do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. o Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio

	przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 lub równoważne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzenia – dokumenty potwierdzające należy załączyć do oferty.
Wdrożenie	Zamawiający wymaga montażu fizycznego serwera wraz z pełną aktualizacją systemu operacyjnego hosta i maszyn wirtualnych/oprogramowania układowego serwera na dzień wdrożenia. Wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania, oraz serwera fizycznego i maszyn wirtualnych które to Wykonawca musi uruchomić na w/w serwerze wg wskazać Zamawiającego na etapie wdrożenia.
Ilość	1 szt.

2. MACIERZ DYSKOWA TYP 1

Nazwa	Minimalne wymagania dla sprzętu
Typ	Macierz dyskowa typ 1 dla Urzędu Gminy Pępowo
Wymagania ogólne	1. Dostarczone urządzenie musi oferować przestrzeń min. 8TB netto powierzchni użytkowej bez uwzględniania mechanizmów protekcji, wymagana możliwość minimum 4-o krotnego zwiększenia pojemności netto w obrębie tego samego urządzenia (przy zachowaniu globalnej deduplikacji w obrębie całej dostępnej przestrzeni dedykowanej do składowania danych) 2. Oferowane urządzenie musi posiadać minimum: • 4 porty Eth 10 Gb/s BaseT • 2 porty Eth 10Gb/s OP wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, deduplikacja na źródle; 3. Dostarczone urządzenie musi umożliwiać dodatkową rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę). Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Skalowanie w przypadku wykorzystywanej przestrzeni warstwy typu Cloud musi stanowić równoważność co najmniej dwukrotnej pojemności netto oferowanego urządzenia (bez uwzględnienia warstwy CLOUD). 4. Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: • CIFS, NFS, • zapewniającym deduplikację na źródle • VTL (po doposażeniu w porty FC)

	5. 6.Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami CIFS, NFS: co najmniej 3 TB/h (dane podawane przez producenta) oraz co najmniej 7 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta). 6. Urządzenie musi pozwalać na jednoczesną obsługę minimum 90 strumieni jednocześnie, w tym • Min. 30 dedykowanymch do zapisu • Min. 30 dedykowanych do odczytu • Min. 30 dedykowanych do replikacji wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. 7. Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia, powyższe wymaganie nie będzie spełnione, jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup'ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu'owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup'owej również muszą być deduplikowane w sposób in-line 8. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków uzywanych do deduplikacji danych określonego typu. 9. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o długości nie większej niż 12 kB.Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie

	może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. 10. Oferowane urządzenie musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całej przestrzeni urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A", nie może zostać ponownie zapisany, jeśli trafi do innej wirtualnej biblioteki „B" w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. 11. Oferowane urządzenie musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całej przestrzeni urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A", nie może zostać ponownie zapisany, jeśli trafi do innej wirtualnej biblioteki „B" w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. 12. Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. 13. Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line) 14. Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane jedną z metod do wyboru: gz, lz.

	15. Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane, dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych. 16. urządzenie musi umożliwiać deduplikację na źródle przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby do oferowanego urządzenia były transmitowane poprzez sieć – LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. Urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwera do urządzenia były transmitowane poprzez sieć tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu 17. W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. 18. Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych. Spełnienie wymagania nie może być ograniczone dla wybranych grup danych ze względu na miejsce składowania czy konkretną retencję. 19. Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych. 20. Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego z oferowanych urządzeń oraz innych urządzeń takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: • jeden do jednego • wiele do jednego • jeden do wielu • kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C). Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania. 21. Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. 22. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych,

	przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. 23. Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. 24. Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. 25. Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej. 26. Oferowane urządzenie musi umożliwiać realizację oraz przechowywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). 27. Urządzenie musi pozwalać na realizację i przechowywanie minimum 300 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia - umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. 28. Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). 29. Urządzenie musi mieć możliwość podziału na minimum 4 logiczne części pracujące równolegle. 30. Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. 31. Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem: • CIFS • NFS • zapewniającym deduplikację na źródle • VTL

	32. Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora): • Możliwość zdjęcia blokady przed upływem ważności danych • Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE, wymagane wsparcie dla norm: SEC 17a-4(f) oraz ISO Standard 15489-1 lub równoważnych) 33. Licencje na blokadę skasowania/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem. Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady, wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). 34. Urządzenie musi weryfikować ewentualne przekłamania (zmianę danych) na poziomie systemu plików. Wymaga się, aby urządzenie weryfikowało sumy kontrolne dla wszystkich fragmentów zapisywanych danych, niezaleznie od używanego interfejsu. 35. Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup'owych w trybie „end-to-end"). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności) 36. Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. 37. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). 38. Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora). Zamawiający zastrzega możliwość prośby o

	dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności. 39. Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. 40. Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas, w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). 41. Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni. 42. Urządzenie musi mieć możliwość zarządzania poprzez • Interfejs graficzny dostępny z przeglądarki internetowej • Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell 43. Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym. 44. Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania. 45. Oferowane urządzenie powinno być objęte wsparciem producenta w okresie minimum 36-u miesięcy, realizowanym w trybie zgłoszeń awarii: 24x7 oraz reakcji on-site NBD.
Wdrożenie oraz szkolenie	1. Wymagana jest konfiguracji dostarczanego oprogramowania backupowego w celu dodania nowego celu backupu za pomocą dedykowanego protokołu dla tego typu urządzeń. Niedozwolony jest standardowy protokół SMB/NFS. 2. Zamawiający wymaga przeszkolenia na etapie wdrożenia min. 1 administratora w zakresie konfiguracji nowych volumenów, ich usuwania, przypisania do hosta, zarządzania migawkami oraz procesu aktualizacji oprogramowania, proces generowania logów dla pomocy technicznej i procesu adresacji nowych interfejsów deduplikatora dla tzw. Frontendu. 3. Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego środowiska serwerowego. 4. Wykonawca wymaga ustawienia adresacji i podłączenie urządzeń zgodnie z wymaganiami Zamawiającego.
Ilość	1 szt.

3. MACIERZ DYSKOWA TYP 2

Nazwa	Minimalne wymagania dla sprzętu
Typ	Macierz dyskowa typ 2 dla Urzędu Gminy Pępowo
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 12 dysków 3.5”
Przestrzeń dyskowa	Zainstalowane: Min. 4x dysk SSD SAS o pojemności min. 3.84TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie min. 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.

Interfejsy	Macierz musi posiadać, co najmniej 8 portów 10Gb iSCSI BaseT (4 porty na kontroler)
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać

	zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International) lub równoważne.

Inne	Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub równoważnymi.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.

	○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania

	○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności

	○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android • Certyfikaty ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: ▪ ISO 27001 lub równoważne. ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization lub równoważne. ▪ CSA Cloud Control Matrix lub równoważne.
Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta na okres min. 36 miesięcy. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. Zamawiający wymaga dołączenia do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia

	awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: • Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. • Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. • Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 lub równoważne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzenia – dokumenty potwierdzające należy załączyć do oferty.
Wdrożenie	• Zamawiający wymaga, aby wykonawca wykonał następujące prace wdrożeniowe: Instalacja fizyczna sprzętu w serwerowi. • Ustawienie adresacji i podłączenie urządzeń zgodnie z wymaganiami Zamawiającego. • Aktualizacja oprogramowania systemowego oraz układowego wdrażanych rozwiązań do najnowszego na dzień wdrożenia • Przygotowanie dokumentacji powdrożeniowej.
Ilość	1 szt.

4. UPS

Nazwa	Minimalne wymagania dla sprzętu

Typ	UPS dla Urzędu Gminy Pępowo
Moc pozorna	min. 20000VA
Moc rzeczywista	min. 20000W
Technologia	on-line (VFI), podwójna konwersja
Sprawność przy pracy sieciowej	minimum 95,5 %
Sprawność przy pracy bateryjnej	minimum 94,5 %
Sprawność w trbie ECO	minimum 98,5 %
Typ obudowy	tower
Wejście	
Napięcie wejściowe	Minimum 3 x 360VAC/380VAC/400VAC/415VAC (3f+N+PE)
Częstotliwość napięcia wejściowego	46~54 Hz lub 56~64 Hz
Zakres napięcia wejściowego	190-520 VAC (3-fazowe) @ 50% obciążenia; 305-478 VAC (3-fazowe) @ 100% obciążenia
Kształt napięcia wyjściowego	sinusoidalny
Czas przełączania sieć – bateria	0ms
Wyjście	
Napięcie wyjściowe	Minimum 3 x 360VAC/380VAC/400VAC/415VAC (3f +N+PE) lub 220/230/240VAC(L+N) ± 1%
Częstotliwość napięcia wyjściowego	50/60 Hz ± 1%
Kształt napięcia wyjściowego na pracy bateryjnej	sinusoidalny
Współczynnik odkształceń prądu wejściowego THD	≦ 2 % (obciążenie liniowe); ≦ 5 % (obciążenie nieliniowe)
Współczynnik szczytu	3:1
Baterie wewnętrzne w UPS lub w zewnętrznym module bateryjnym	minimum 12V 9Ah; szczelne, bezobsługowe
Czas podtrzymania dla obciążenia 14kW - przy zastosowaniu wyłącznie baterii wewnątrz UPSa	minimum 5 minut
Pozostałe	
Prąd ładowania baterii (max)	12A
Czas ładowania do 90% pojemności baterii	maksymalnie 9h

Wejście zasilania	listwa zaciskowa / terminal śrubowy
Wyjście zasilania	listwa zaciskowa / terminal śrubowy
Przeciążalność w trybie sieciowym AC	100%~110%:10min; 110%~130%:1min; >130%:1s
Sygnalizacja	Dotykowy wyświetlacz LCD z menu w języku polskim
Informacje konfigurowane/wyświetlane na panelu LCD	Możliwość kalibracji prądu ładowania
	Pomiar obciążenia na każdej fazie indywidualnie
	Monitorowanie współczynnika mocy PF na każdej fazie
Interfejs komunikacyjny - każdy jako osobne gniazdo/złącze	Minimum RS232, USB
Zabezpieczenia	minimum przeciwzwarciowe, przeciwprzepięciowe, przeciążeniowe
Złącze EPO	wymagane
Gwarancja	minimum 24 miesiące gwarancji producenta na elektronikę i min. 12 miesięcy gwarancji producenta na akumulatory;
	naprawa w maksymalnie 14 dni roboczych
	serwis realizowany w systemie onsite - w miejscu instalacji
Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS
	wsparcie dla systemów: Windows, Linux
	jedno wspólne oprogramowanie do zarzadzania UPSami 1-fazowymi i 3-fazowymi tego samego producenta
	wymagane techniczne wsparcie producenta (telefoniczne oraz mailowe) w języku polskim.
Wymagania dodatkowe	Możliwość monitorowania i konfiguracji UPS przez przeglądarkę WWW
Oświadczenia / dokumenty	deklaracja zgodności CE lub norm równoważnych
	Należy załączyć do oferty oświadczenie producenta o posiadaniu przez oferenta statusu Autoryzowanego Partnera - mającego wiedzę w zakresie doboru i sprzedaży zasilania gwarantowanego (UPS)
Usługi	W ramach dostawy wymagane jest dodatkowo: - Podłączenie do przygotowanej instalacji elektrycznej (wykonanej zgodnie z wytycznymi producenta) przez Autoryzowany Serwis Producenta uwzględniające podłączenie wejścia zasilania do terminala śrubowego w UPS. - Pierwsze uruchomienie. - Szkolenie z obsługi. - Dostawa kurierem do poziomu zero bez wniesienia
Ilość	1 szt.

5. ZARZĄDZALNE URZĄDZENIA SIECIOWE Z OBSŁUGĄ VLAN, MACSEC, STANDARDU 802.1X - TYP 1

Nazwa	**Minimalne wymagania dla sprzętu**

Typ	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X - typ 1 dla Urzędu Gminy Pępowo
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona pasywnie.
Porty	Minimum 24 porty 10/100/1000Mbps RJ45, minimum 4 porty SFP+ 10GbE, Minimum 1 port konsolowy Minimum 1 port USB Obsługa modułów SFP+: 10GbE, SR, LR, ER
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity min. 128 Gbps Forwarding rate min. 95Mpps Pamięć flash min. 512MB Bufor pakietów min. 1.5MB
Funkcjonalność warstwy II	Obsługa minimum 4093 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa minimum 8 grup LACP i minimum 16 portów fizycznych per grupa
Funkcjonalność warstwy III	Obsługa minimum 990 wpisów routingu statycznego IPv4
Inne Funkcjonalności	Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP Minimum 1024 list kontroli dostępu Minimum 126 instancje STP
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.3ad Link Aggregation with LACP 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIv2 2011 IP MIB 2012 TCP MIB

	2013 UDP MIB 2233 Interfaces Group using SMIv2 2618 RADIUS Authentication MIB 2863 Interfaces MIB 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
Wdrożenie	Zamawiający wymaga aby wykonawca dokonał wdrożenia o zakresie min,: • Demontaż starych przełączników • Instalacja w szafach rack zamawiającego nowych przełączników • Aktualizacja oprogramowania przełączników do najnowszej dostępnej wersji • Podstawowa konfiguracja przełączników tj. interfejsy do zarządzania, konto administracyjne • Konfiguracja na przełącznikach protokołu typu RSTP wraz z oferowanymi przez dany sprzęt zabezpieczeniami typu Root Guard, Loop Guard, BPDU Guard w sposób zgodny z tzw. dobrymi branżowymi praktykami oraz trybu portfast/edge port na portach dla urządzeń końcowych Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego środowiska.
Gwarancja	Co najmniej 36 miesięcy gwarancji producenta
Ilość	6 szt.

6. ZARZĄDZALNE URZĄDZENIA SIECIOWE Z OBSŁUGĄ VLAN, MACSEC, STANDARDU 802.1X - TYP 2

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X - typ 2 dla Urzędu Gminy Pępowo
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona pasywnie.

Porty	Minimum 24 porty 10/100/1000Mbps RJ45 POE, minimum 4 porty SFP+ 10GbE, Minimum 1 port konsolowy Minimum 1 port USB Obsługa modułów SFP+: 10GbE, SR, LR, ER
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity min. 128 Gbps Forwarding rate min. 95Mpps Pamięć flash min. 512MB Bufor pakietów min. 1.5MB Budżet POE min. 195W
Funkcjonalność warstwy II	Obsługa minimum 4093 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa minimum 8 grup LACP i minimum 16 portów fizycznych per grupa
Funkcjonalność warstwy III	Obsługa minimum 990 wpisów routingu statycznego IPv4
Inne Funkcjonalności	Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP Minimum 1024 list kontroli dostępu Minimum 126 instancje STP
Zgodność z protokołami	802.1AB LLDP 802.3af 802.3at 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.3ad Link Aggregation with LACP 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIv2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB

	2233 Interfaces Group using SMIv2 2618 RADIUS Authentication MIB 2863 Interfaces MIB 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
Wdrożenie	Zamawiający wymaga aby wykonawca dokonał wdrożenia o zakresie min,: • Demontaż starych przełączników • Instalacja w szafach rack zamawiającego nowych przełączników • Aktualizacja oprogramowania przełączników do najnowszej dostępnej wersji • Podstawowa konfiguracja przełączników tj. interfejsy do zarządzania, konto administracyjne • Konfiguracja na przełącznikach protokołu typu RSTP wraz z oferowanymi przez dany sprzęt zabezpieczeniami typu Root Guard, Loop Guard, BPDU Guard w sposób zgodny z tzw. dobrymi branżowymi praktykami oraz trybu portfast/edge port na portach dla urządzeń końcowych Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego środowiska.
Gwarancja	Co najmniej 36 miesięcy gwarancji producenta
Ilość	1 szt.

7. ZARZĄDZALNE URZĄDZENIA SIECIOWE Z OBSŁUGĄ VLAN, MACSEC, STANDARDU 802.1X - TYP 3

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X - typ 1 dla Gminnego Ośrodka Pomocy Społecznej w Pępowie
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona pasywnie.
Porty	Minimum 48 porty 10/100/1000Mbps RJ45, minimum 4 porty SFP+ 10GbE, Minimum 1 port konsolowy

	Minimum 1 port USB Obsługa modułów SFP+: 10GbE, SR, LR, ER
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity min. 128 Gbps Forwarding rate min. 95Mpps Pamięć flash min. 512MB Bufor pakietów min. 1.5MB
Funkcjonalność warstwy II	Obsługa minimum 4093 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa minimum 8 grup LACP i minimum 16 portów fizycznych per grupa
Funkcjonalność warstwy III	Obsługa minimum 990 wpisów routingu statycznego IPv4
Inne Funkcjonalności	Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP Minimum 1024 list kontroli dostępu Minimum 126 instancje STP
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.3ad Link Aggregation with LACP 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIv2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2233 Interfaces Group using SMIv2 2618 RADIUS Authentication MIB 2863 Interfaces MIB 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2

	3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
Gwarancja	Co najmniej 36 miesięcy gwarancji producenta
Ilość	1 szt.

8. OPROGRAMOWANIE ANTYWIRUSOWE

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Oprogramowanie antywirusowe dla Urzędu Gminy w Pępowie
Wymagania podstawowe	Zamawiający posiada licencję ESET PROTECT Essential ON-PREM (obejmującą 38 stanowisk). Zamawiający wymaga przedłużenia bieżącej licencji do daty 30-06-2026 oraz rozszerzenia jej do wersji ESET PROTECT Entry. Zamawiający dopuszcza dostarczenie oprogramowania równoważnego (wymianę w/w oprogramowania) spełniającego poniższe wymagania minimalne. Ponadto, w przypadku dostawy oprogramowania równoważnego Zamawiający wymaga dodatkowo: • Wdrożenia • skonfigurowania dla wszystkich użytkowników • przeszkolenia administratorów z dostarczonego oprogramowania, wg ustaleń z Zamawiającym.
OPIS RÓWNOWAŻNOŚCI	
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 wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 7. 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.

	8. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 9. rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 10. 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. 11. 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 32 i 64-bitową systemu Windows. 3. Rozwiązanie musi wspierać architekturę ARM64. 4. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 6. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 7. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 8. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 9. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 10. 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. 11. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 12. 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). 13. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 14. 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. 15. 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. 16. 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. 17. 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. 18. 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. 19. 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. 20. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 21. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 22. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 23. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 24. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

	• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 25. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 26. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 27. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 28. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 29. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 30. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 31. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
Ochrona serwera	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu 2. Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise 3. Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux. 4. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 6. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 7. 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. 8. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

	9. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 10. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 11. Dodatkowe wymagania dla ochrony serwerów Windows: 12. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 13. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 14. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 15. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 16. 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. 17. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 18. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 19. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 20. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. 21. Dodatkowe wymagania dla ochrony serwerów Linux: 22. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 23. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 24. 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.
Ilość	1 szt.

9. OPROGRAMOWANIE DO WYKONYWANIA KOPII ZAPASOWYCH

Nazwa	**Minimalne wymagania dla oprogramowania**

Typ	Oprogramowanie do wykonywania kopii zapasowych dla Urzędu Gminy w Pępowie
Wymagania ogólne	• Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych chmurowych pamięci masowych i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. • 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 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 zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. • Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach chmurowych oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. • Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania • Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) • Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu

	• Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API • 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 posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. • Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej • Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora) • Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS) • Oprogramowanie musi posiadać integracje z systemami typu SIEM • Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
Wymagania RPO	• Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej • Oprogramowanie musi wykorzystywać mechanizmy 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 z dokładnością do pojedynczego datastoru • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. • Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

	• Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) • Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi dostarczanymi w ramach postepowania. • Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. • 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 mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. • 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, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. • Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV 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 pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do platform chmurowych. • Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień 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 natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. • Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM • 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, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych

	witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. • 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 wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. • 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. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) • Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. • 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 umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware • Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania • Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków • Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Środowiska fizyczne	• Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego • Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych • Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: • Rozwiązanie musi wspierać system operacyjny macOS • Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix • Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) • Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster • Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów • Rozwiązanie musi wspierać backup podłączonych dysków USB • Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym • Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) • Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone • Rozwiązanie musi wspierać kontrolę pasma sieciowego • Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych • Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN • Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft • Rozwiązanie musi wspierać technologię BitLocker • Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania • Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej

	• Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych • Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. • Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do platform chmurowych. • Rozwiązanie musi wspierać szyfrowanie • Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne • Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego • Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej • Rozwiązanie musi wspierać tworzenie wielu zadań backupowych • 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 6.x, 7.x oraz 8.0 – 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 2012, 2012R2, 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 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
Raportowanie	• System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie • System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 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 wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. • 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
Licencja	Zamawiający wymaga dostarczenia licencji bezterminowej dla min. 5 instancji wraz ze wsparciem producenta na okres do 30.06.2026
Ilość	1 szt.

IV. CZĘŚĆ NR 3

1. OPROGRAMOWANIE SIEM SECURITY INFORMATION AND EVENT MANAGEMENT

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie SIEM Security Information and Event Management dla Urzędu Gminy w Pępowie
Wymagania ogólne	Wymagane jest dostarczenie oprogramowania posiadającego poniższą funkcjonalność:

	• Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń: • Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego wirtualna maszyna. • Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (usługą katalogową) lub ręcznie przez definiowanie kont w samym rozwiązaniu. • System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514. • System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport. • System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z dowolną przeglądarką WWW. • System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego. • System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów). W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń: • Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynie wirtualne. • Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.

	• Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
	• Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
	• Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:
	  • Urządzenie klasy UTM
	  • Przełączniki zarządzalne
	  • Serwery fizyczne
	  • Serwery wirtualizacji
	  • stacje roboczych
	  • aplikację centralnego zarządzania posiadanego antywirusa
	  • aplikację do monitorowania infrastruktury informatycznej dla Zamawiającego
	• Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
	• Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.
	• Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
	• Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
	• Konfiguracja wysyłania powiadomień poprzez maila w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
	• Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.

Gwarancja i asysta techniczna	Zamawiający wymaga, aby Wykonawca w czasie do 30.06.2026 od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu. Zamawiający wymaga, aby Wykonawca w okresie do 30.06.2026 od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów. Zamawiający wymaga, aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00. Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji

	będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.
Ilość	1 szt.

V. CZĘŚĆ NR 4

1. OPROGRAMOWANIE MOBILE DEVICE MANAGEMENT

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie Mobile Device Management dla Urzędu Gminy w Pępowie
Wymagania ogólne	Wymagania minimalne dla architektury i serwera: 1. System musi umożliwiać instalację na maszynie wirtualnej lub fizycznej Zamawiającego. 2. System MDM musi posiadać dokumentację określającą wymagania maszyny wirtualnej lub fizycznej w zależności od ilości urządzeń do niej dołączonych. 3. Dokumentacja Systemu MDM musi zawierać wszystkie niezbędne informacje odnośnie wymagań sieciowych dla Systemu, w szczególności opis konfiguracji sieciowej opartej na ruchu przychodzącym/wychodzącym na poszczególnych portach. 4. System MDM nie może wymagać dodatkowych licencji dla baz danych. 5. System MDM nie może wymagać dodatkowych licencji dla systemów operacyjnych. 6. System MDM musi być kompatybilny z systemem operacyjnym posiadającym ważne wsparcie dla aktualizacji bezpieczeństwa przynajmniej w okresie dwóch najbliższych lat. 7. System MDM musi oferować wsparcie dla backupu maszyn wirtualnych (snapshot, checkpoint). 8. Konsola Systemu MDM musi być dostępna z poziomu przeglądarki. 9. Konsola Systemu MDM musi być dostępna w języku polskim. 10. Konsola Systemu MDM musi być dostępna w jasny i ciemnym motywie kolorystycznym. 11. Konsola Systemu MDM musi oferować możliwość wymuszenia pojedynczej sesji logowania na koncie administratora. 12. Konsola Systemu MDM musi rejestrować udane i nieudane próby logowania na koncie administratora. 13. System MDM musi oferować obsługę zmiennych globalnych służących do parametryzacji i personalizacji konfiguracji zarządzanej kierowanej w urządzeń. 14. System MDM musi oferować obsługę zmiennych globalnych na poziomie użytkownika, urządzenia, kart SIM oraz certyfikatów. 15. System MDM musi oferować wbudowane centrum certyfikacji. 16. System MDM musi oferować wbudowany VPN. 17. System MDM musi oferować wsparcie dla protokołu SCEP. 18. System MDM musi oferować wsparcie dla Android Enterprise

	19. System MDM musi oferować wsparcie dla Apple Business Manager (dawniej Apple DEP). 20. System MDM musi oferować wsparcie dla Apps and Books (dawniej Apple VPP). 21. System MDM musi oferować wsparcie dla Knox Mobile Enrollment. 22. System MDM musi oferować wsparcie dla Android zero-touch Enrollment. 23. System MDM musi oferować systemowe narzędzie do backupu serwera. 24. System MDM musi oferować wsparcie dla Active Directory. 25. System MDM musi oferować wsparcie dla LDAP. 26. System MDM musi ofertować automatyczny onboarding i offboarding użytkowników. 27. System MDM musi oferować wsparcie dla Azure Active Directory. 28. System MDM musi oferować logowanie jednokrotne (SSO) przy pomocy Azure Active Directory. 29. System MDM musi oferować automatyczną synchronizację użytkowników z usług katalogowych AD/LDAP/AAD. 30. System MDM musi oferować wsparcie dla Microsoft Exchange. 31. System MDM musi oferować wsparcie dla protokołów ActiveSync, POP, IMAP. 32. System MDM musi oferować mechanizm zabezpieczający dostęp do poczty elektronicznej weryfikowany na podstawie dotykowego składnika np. certyfikat użytkownika. 33. System MDM musi oferować dodawanie aplikacji z pliku (aplikacje typu in-house). 34. System MDM musi oferować import aplikacji ze sklepu z aplikacjami Google Play. 35. System MDM musi oferować import aplikacji ze sklepu z aplikacjami iTunes. 36. System MDM musi oferować dodawanie aplikacji z zewnętrznego zasobu. 37. System MDM musi oferować stosowanie konfiguracji zarządzanej dla aplikacji Android. 38. System MDM musi oferować stosowanie konfiguracji zarządzanej dla aplikacji iOS. 39. System MDM musi oferować stosowanie konfiguracji zarządzanej dla aplikacji typu in-house. 40. System MDM musi oferować konfiguracje ACL dla konsoli. 41. System MDM musi oferować możliwość zmiany motywów konsoli (główny kolor, logo, favicon). 42. System MDM musi oferować uwierzytelnianie dwuskładnikowe dla użytkowników konsoli. 43. System MDM musi oferować wbudowany audyt integralności danych i bezpieczeństwa serwera. 44. System MDM musi obsługiwać wysyłanie niestandardowych profili konfiguracyjnych do urządzeń iOS. 45. System MDM musi obsługiwać wysyłanie niestandardowych poleceń do urządzeń iOS.

	46. System MDM musi gromadzić logi audytowe aplikacji. 47. System MDM musi gromadzić informacje na temat wykonanych akcji wewnątrz systemu. 48. System MDM musi gromadzić logi sieciowe aplikacji. 49. System MDM musi oferować konfigurowalną lokalizacje Google Play i App Store. 50. System MDM musi oferować możliwość włączenia dostępu do całej treści zarządzanego sklepu Google Play bez konieczności logowania oraz nałożenie białej lub czarnej listy aplikacji. 51. System MDM musi oferować możliwość przejęcia kontroli zdalnej nad urządzeniem. 52. System MDM musi umożliwiać wykorzystanie klawiatury komputera do wpisywania tekstu na urządzeniu, podczas przejmowania kontroli zdalnej nad urządzeniem. 53. System MDM musi oferować automatyczne i manualne aktualizacje serwera. 54. System MDM musi oferować możliwość aktywowania użytkownika serwisowego celem sesji zdalnej adresowanej dla działu wsparcia producenta. 55. System MDM musi oferować możliwość przypisywania konfiguracji w sposób dynamiczny np. Na podstawie parametrów urządzenia. III. Wspierane urządzenia mobilne 1. Android 8.0 i nowszy. 2. iOS 13 i nowszy. 3. Windows 10/11 Pro/Enterprise. 4. MacOS 11 i nowszy IV. Rejestracja urządzeń w Systemie MDM 1. Rejestracja za pomocą aplikacji poprzez podanie loginu i hasła lub skanu kodu QR. 2. Rejestracja za pomocą kodu QR. 3. Rejestracja za pomocą tagów NFC. 4. Automatyczne dodawanie urządzenia do systemu. 5. Automatyczne dodawanie urządzenia do systemu i powiązanie z przypisanym użytkownikiem. 6. Rejestracja bez użytkownika. 7. Rejestracja z wykorzystaniem Knox Mobile Enrollment. 8. Rejestracja z wykorzystaniem Apple Business Manager. 9. Rejestracja z wykorzystaniem Android zero-touch. 10. Rejestracja za pomocą kodów QR oraz tagów NFC musi ofertować możliwość zapisania danych sieci WiFi. V. Pobierane informacje o zarządzanym urządzeniu 1. Informacja o producencie. 2. Informacja o modelu. 3. Informacja o systemie operacyjny. 4. Informacja o stanie baterii. 5. Informacja o pamięć wewnętrznej.

	6. Informacja o pamięci RAM. 7. Informacja o procesorze. 8. Informacja o operatorze używanych kart SIM. 9. Informacja o język urządzenia. 10. Informacja o szyfrowanie danych na urządzeniu. 11. Informacja o IP sieci komórkowej. 12. Informacja o IP sieci Wi-Fi. 13. Informacja o adresie MAC sieci Wi-Fi. 14. Informacja o SSID podłączonej sieci Wi-Fi. 15. Informacja o ICCID używanych kart SIM. 16. Informacja o numerze telefonu. 17. Informacja o IMEI gniazd kart SIM. 18. Informacja o numerze seryjnym. 19. Informacja o ostatnim kontakcie urządzenia z serwerem. 20. Informacja o wykorzystaniu karty SD. 21. Informacja o dostępności aktualizacji systemu operacyjnego. 22. Informacja o aplikacjach na urządzeniu wraz z wersją aplikacji. 23. System MDM musi oferować możliwość wykonania raportu wykorzystania pamięci urządzenia. 24. System MDM musi oferować możliwość wykonania raportu wykorzystania danych mobilnych na urządzeniu. 25. System MDM musi oferować możliwość wykonania raportu wykorzystania danych przez Wi-Fi na urządzeniu. 26. System MDM musi oferować możliwość wykonania raportu wykorzystania aplikacji na urządzeniu. VI. Wspierane konfiguracje urządzeń 1. System MDM musi oferować możliwość blokady urządzenia. 2. System MDM musi oferować możliwość wykonania zdjęcia podczas blokady urządzenia. 3. System MDM musi oferować możliwość resetu hasła. 4. System MDM musi oferować możliwość zmiany hasła przez administratora. 5. System MDM musi oferować możliwość przywrócenia urządzeń do ustawień fabrycznych. 6. System MDM musi oferować możliwość usunięcia danych służbowych z urządzeń. 7. System MDM musi oferować możliwość zablokowania ekranu urządzenia. 8. System MDM musi oferować możliwość wysłania notyfikacji. 9. System MDM musi oferować możliwość wysłania alarmu wraz z potwierdzeniem jego otrzymania i przeczytania. 10. System MDM musi oferować możliwość przekierowania połączeń na dowolny podany numer telefonu, 11. System MDM musi oferować możliwość restartu urządzenia. 12. System MDM musi oferować możliwość eksportu SMS. 13. System MDM musi oferować możliwość eksportu kontaktów. 14. System MDM musi oferować możliwość eksportu dziennika połączeń.

	15. System MDM musi oferować możliwość eksportu logów audytowych z urządzenia. 16. System MDM musi oferować możliwość lokalizacji urządzeń na żądanie. 17. System MDM musi oferować możliwość lokalizacji urządzeń w interwałach czasowych. 18. System MDM musi oferować możliwość lokalizacji urządzeń w ruchu. 19. System MDM musi oferować możliwość zbierania historia lokalizacji urządzeń. 20. System MDM musi oferować możliwość zastosowania ograniczeń czasowych dla zbierania lokalizacji urządzeń. 21. System MDM musi oferować możliwość filtrowania urządzeń po ich lokalizacji. 22. System MDM musi oferować możliwość zablokowania i odblokowania aplikacji na urządzeniu. 23. System MDM musi oferować możliwość uruchomienia aplikacji na urządzeniu. 24. System MDM musi ofertować możliwość zarządzanej konfiguracji dla aplikacji ze sklepu Google Play oraz App Store. 25. System MDM musi ofertować możliwość zarządzanej konfiguracji dla aplikacji z pliku. 26. System MDM musi oferować możliwość wysłania konfiguracji aplikacji na urządzenia. 27. System MDM musi oferować możliwość usunięcie aplikacji z urządzenia. 28. System MDM musi oferować możliwość backupu SMS i MMS. 29. System MDM musi oferować możliwość backupu kontaktów. 30. System MDM musi oferować możliwość backupu dziennika połączeń. 31. System MDM musi oferować możliwość wykonania kopii zapasowej urządzenia Android bez konieczności rejestracji urządzenia (samodzielny system kopii zapasowej). 32. System MDM musi oferować możliwość instalacji aplikacji ze sklepu oraz z pliku. 33. System MDM musi oferować możliwość cichej instalacji aplikacji. 34. System MDM musi oferować możliwość instalacji skonfigurowanych aplikacji. 35. System MDM musi oferować możliwość opóźnienia instalacji aplikacji ze sklepu Play. 36. System MDM musi oferować możliwość konfiguracji warunków instalacji aplikacji ze sklepu Play takich jak podłączenie do WiFI, minimalna wersja kodowa aplikacji, instalacja tylko w stanie bezczynności, instalacja tylko podczas ładowania urządzenia. 37. System MDM musi umożliwiać powiadomienie użytkownika końcowego o przypisaniu nowej konfiguracji aplikacji. 38. System MDM musi umożliwiać wyczyszczenie danych aplikacji przed przypisanem nowej konfiguracji aplikacji. 39. System MDM musi oferować możliwość zarządzania uprawnieniami aplikacji.

	40. System MDM musi oferować możliwość uruchomienia służbowego sklepu z aplikacjami. 41. System MDM musi oferować możliwość włączenie Activation Lock. 42. System MDM musi oferować możliwość wyłączenie Activation Lock. 43. System MDM musi oferować możliwość dostarczenia konfiguracji ActiveSync. 44. System MDM musi oferować możliwość konfiguracji ActiveSync z szyfrowaniem S/MIME. 45. System MDM musi oferować możliwość dostarczenia konfiguracji IMAP/POP. 46. System MDM musi oferować możliwość konfiguracji Wi-Fi. 47. System MDM musi oferować możliwość konfiguracji Enterprise Wi-Fi. 48. System MDM musi oferować możliwość konfiguracji SCEP. 49. System MDM musi oferować możliwość dostarczenia certyfikatu na urządzenie. 50. System MDM musi oferować możliwość konfiguracji VPN w tym VPN per aplikacja. 51. System MDM musi oferować możliwość stworzenia białej i czarnej listy aplikacji dla przestrzeni służbowej. 52. System MDM musi oferować możliwość stworzenia białej i czarnej listy aplikacji dla przestrzeni prywatnej. 53. System MDM musi oferować możliwość stworzenia białej lista aplikacji podczas przemieszczania się urządzenia. 54. System MDM musi oferować możliwość dostarczenia i zarządzania kontaktami służbowymi. 55. System MDM musi oferować możliwość dostarczenia dokumentów służbowych 56. System MDM musi oferować możliwość pobierania udostępnionych plików automatycznie 57. System MDM musi oferować możliwość konfiguracji tapety. 58. System MDM musi oferować możliwość dostarczenia konfiguracji APN. 59. System MDM musi oferować możliwość konfiguracji trybu kiosk – pojedyncza aplikacja i wiele aplikacji. 60. System MDM musi oferować możliwość konfiguracji trybu kiosk - wiele aplikacji z logowaniem użytkownika do urządzenia. 61. System MDM musi oferować możliwość konfiguracji aplikacji „OEM Config” w szczególności Knox Service Plugin. 62. System MDM musi oferować możliwość zarządzania aktualizacjami systemu operacyjnego Android. 63. System MDM musi oferować możliwość ustawienia wymagań minimalnych hasła urządzenia. 64. System MDM musi oferować możliwość ustawienia wymagań minimalnych hasła w przestrzeni służbowej. 65. System MDM musi oferować możliwość użycia biometrii do odblokowania urządzenia.

	66. System MDM musi oferować możliwość użycia biometrii do odblokowania przestrzeni służbowej. 67. System MDM musi oferować możliwość wyświetlania wiadomości na zablokowanym ekranie. 68. System MDM musi oferować możliwość zablokowania Bluetooth. 69. System MDM musi oferować możliwość wykrywania i reagowania na Root. 70. System MDM musi oferować możliwość wykrywania i reagowania na włączone debugowanie przez USB. 71. System MDM musi oferować możliwość wykrywania i reagowania na brak zaszyfrowania urządzenia. 72. System MDM musi oferować możliwość wykrywania i reagowania na włączone opcje developerskie. 73. System MDM musi oferować możliwość wykrywania i reagowania na podatność BlueBorne. 74. System MDM musi oferować możliwość wykrywania i reagowania na wyłączony SELinux. 75. System MDM musi oferować możliwość wykrywania i reagowania na niezaufanych administratorów urządzenia. 76. System MDM musi oferować możliwość wykrywania i reagowania na instalacje niedozwolonej aplikacji. 77. System MDM musi oferować możliwość wykrywania i reagowania na połączenie do niezabezpieczonej sieci Wi-Fi. 78. System MDM musi oferować możliwość wykrywania i reagowania na zmianę konfiguracji DNS. 79. System MDM musi oferować możliwość wykrywania i reagowania na zmianę konfiguracji Proxy. 80. System MDM musi oferować możliwość wykrywania i reagowania na zmianę konfiguracji Gateway. 81. System MDM musi oferować możliwość zablokowania użycia danych mobilnych w roamingu. 82. System MDM musi oferować rejestrację urządzeń Android w usłudze Azure Active Directry. 83. System MDM musi oferować wsparcie obsługi dostępu warunkowego (Conditional Access) do zasobów Office365 dla urządzeń Android. 84. System MDM musi oferować możliwość zablokowania tetheringu i mobilnych hotspotów. 85. System MDM musi oferować możliwość zablokowania dodawania nowych konfiguracji Wi-Fi. 86. System MDM musi oferować możliwość zablokowania podłączania nośników fizycznych. 87. System MDM musi oferować możliwość zablokowania połączeń wychodzących. 88. System MDM musi oferować możliwość zablokowania SMS. 89. System MDM musi oferować możliwość zablokowania transferu plików przez USB.

	90. System MDM musi oferować możliwość ustawiania metod wprowadzania danych. 91. System MDM musi oferować możliwość zarządzania usługami lokalizacji. 92. System MDM musi oferować możliwość określania sposobu nadawania uprawnień aplikacji. 93. System MDM musi oferować możliwość określania sposobu aktualizacji aplikacji ze sklepu Google Play. 94. System MDM musi oferować możliwość zablokowania dodawania użytkowników nowych użytkowników do urządzenia. 95. System MDM musi oferować możliwość zablokowania zrzutów ekranu. 96. System MDM musi oferować możliwość zablokowania opcji deweloperskich. 97. System MDM musi oferować możliwość zablokowania trybu awaryjnego. 98. System MDM musi oferować możliwość zablokowania przywracania urządzeń do ustawień fabrycznych przez użytkownika 99. System MDM musi oferować możliwość zablokowania dodawania nowych kont Google. 100. System MDM musi oferować możliwość zablokowania instalowania aplikacji z nieznanych źródeł. 101. System MDM musi oferować możliwość wymuszania cyklicznego połączenia urządzenia z serwerem. 102. System MDM musi oferować możliwość wykonania akcji w przypadku przekroczenia czasu nieaktywności. 103. System MDM musi oferować możliwość zablokowania Smart Lock. 104. System MDM musi oferować możliwość zablokowania OTG przez USB. 105. System MDM musi oferować możliwość wymuszenia stałego adresu MAC podczas łączenia się z siecią WiFi. 106. System MDM musi oferować możliwość zablokowania mikrofonu. 107. System MDM musi oferować możliwość zablokowania zmian tapety. 108. System MDM musi oferować możliwość SIM pinning (ochrona przed użyciem służbowej kart SIM w urządzeniu innym niż służbowe). 109. System MDM musi oferować możliwość zablokowania FaceTime. 110. System MDM musi oferować możliwość zablokowania zrzutów ekranu i nagrywania ekranu. 111. System MDM musi oferować możliwość zablokowania AirDrop. 112. System MDM musi oferować możliwość zablokowania iMessage. 113. System MDM musi oferować możliwość zablokowania usług Apple Music. 114. System MDM musi oferować możliwość zablokowania usługi radio. 115. Zablokowanie głosowego wybierania numeru na zablokowanym ekranie 116. System MDM musi oferować możliwość zablokowania Siri. 117. System MDM musi oferować możliwość zablokowania iBooks. 118. System MDM musi oferować możliwość zablokowania zakupów w aplikacji. 119. System MDM musi oferować możliwość zablokowania hasła iTunes podczas zakupów. 120. System MDM musi oferować możliwość zablokowania iCloud backup.

	121. System MDM musi oferować możliwość zablokowania synchronizacji dokumentów w iCloud. 122. System MDM musi oferować możliwość zablokowania Keychain w iCloud. 123. System MDM musi oferować możliwość zablokowania backupu iCloud aplikacjach zarządzanych. 124. System MDM musi oferować możliwość zablokowania backupu służbowych książek. 125. System MDM musi oferować możliwość zablokowania dzielenia zdjęć z iCloud. 126. System MDM musi oferować możliwość zablokowania biblioteki zdjęć z iCloud. 127. System MDM musi oferować możliwość zablokowania My Photo Stream. 128. System MDM musi oferować możliwość wymuszenia ograniczonego śledzenia reklam. 129. System MDM musi oferować możliwość zablokowania niezaufanych certyfikatów TLS. 130. System MDM musi oferować możliwość zablokowania instalacji profili konfiguracyjnych. 131. System MDM musi oferować możliwość zablokowania modyfikowania kont. 132. System MDM musi oferować możliwość zablokowania zmiany nazwy urządzenia. 133. System MDM musi oferować możliwość zablokowania Handoff 134. System MDM musi oferować możliwość zablokowania wyników wyszukiwania z Internetu w Spotlight. 135. System MDM musi oferować możliwość zablokowania wysyłania danych diagnostycznych Apple. 136. System MDM musi oferować możliwość zablokowania wykrywania Apple Watch. 137. System MDM musi oferować możliwość zablokowania parowania Apple Watch. 138. System MDM musi oferować możliwość zablokowania klawiatury predykcyjnej. 139. System MDM musi oferować możliwość zablokowania skrótów klawiszowych. 140. System MDM musi oferować możliwość zablokowania autokorekty. 141. System MDM musi oferować możliwość zablokowania sprawdzania pisowni. 142. System MDM musi oferować możliwość zablokowania Control Center na ekranie blokady. 143. System MDM musi oferować możliwość zablokowania Notification Center na ekranie blokady. 144. System MDM musi oferować możliwość zablokowania widoku Today na ekranie blokady. 145. System MDM musi oferować możliwość zablokowania AirPrint.

	146. System MDM musi oferować możliwość zablokowania przechowywania poświadczeń AirPrint. 147. System MDM musi oferować możliwość zablokowania wykrywania iBeacon w AirPrint. 148. System MDM musi oferować możliwość zablokowania dyktowania. 149. System MDM musi oferować możliwość zablokowania modyfikacji eSIM. 150. System MDM musi oferować możliwość zablokowania autouzupełniania haseł. 151. System MDM musi oferować możliwość zablokowania pytania o hasło z pobliskich urządzeń. 152. System MDM musi oferować możliwość opóźnienia aktualizacji systemu operacyjnego. 153. System MDM musi oferować możliwość wymuszenia korzystania z Wi-Fi. 154. System MDM musi oferować możliwość zablokowania iTunes. 155. System MDM musi oferować możliwość zablokowania News. 156. System MDM musi oferować możliwość zablokowania Podcasts. 157. System MDM musi oferować możliwość zablokowania Game Center. 158. System MDM musi oferować możliwość zablokowania Safari. 159. System MDM musi oferować możliwość konfiguracji Safari. 160. System MDM musi oferować możliwość zablokowania App Store. 161. System MDM musi oferować możliwość zablokowania klawiatury QuickPath. 162. System MDM musi oferować możliwość zablokowania dostępu Files do dysków sieciowych. 163. System MDM musi oferować możliwość zablokowania dostępu Files do dysków USB. 164. System MDM musi oferować możliwość zablokowania Find My Device. 165. System MDM musi oferować możliwość zablokowania Find My Friends. 166. System MDM musi oferować możliwość zablokowania usuwania aplikacji systemowych. 167. System MDM musi oferować możliwość filtrowania treści w Safari.
Wymagania dodatkowe	W ramach dostawy Zamawiający wymaga dodatkowo wdrożenie rozwiązania, w infrastrukturze teleinformatycznej Zamawiającego, systemu do zarządzania flotą urządzeń mobilnych, zwanego dalej Systemem MDM (Mobile Device Management) oraz przeprowadzenia online szkolenia technicznego dla Administratorów po stronie Zamawiającego w zakresie obsługi, konfiguracji oraz administracji Systemem MDM.
Licencje	Zamawiający wymaga dostarczenia: • niewyłącznych licencji umożliwiających dołączenie ilości urządzeń mobilnych Zamawiającego, do konsoli Systemu MDM • licencji dożywotnia z wsparciem na okres 1 roku dla 32 urządzeń • wsparcie w języku polskim w ramach udzielonej licencji oraz konsola w języku polskim
Ilość	1 szt.

VI. CZĘŚĆ NR 5

1. OPROGRAMOWANIE DO MONITOROWANIA INFRASTRUKTURY INFORMATYCZNEJ

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do monitorowania infrastruktury informatycznej dla Urzędu Gminy w Pępowie
Wymagania ogólne	W ramach dostawy Zamawiający wymaga dostarczenia licencji na oprogramowanie dla 40 użytkowników wraz z wparciem technicznym na minimum 12 miesięcy, spełniającym poniższe wymagania minimalne.
Inwentaryzacja sprzętu i Oprogramowania	Dostarczone oprogramowanie powinno spełniać minimalne wymagania: Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. Informacja o zainstalowanych aplikacjach oraz aktualizacjach co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. Zbieranie informacji w zakresie zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP Posiadanie możliwości wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. Możliwość odczytania numeru seryjnego (klucze licencyjne). Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. Możliwość przeglądu informacji o konfiguracji systemu, tj. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań.
Monitorowanie Aktywności	Oprogramowanie powinno umożliwiać monitorowanie aktywności oraz posiadać min. Funkcjonalności: Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach. Monitorowanie rzeczywistego użytkowania programów (procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt). Monitorowania transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika). Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen. Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji

	tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
Ochrona danych	Zarządzanie prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. Autoryzowanie urządzeń firmowych: pendrive'ów, dysków zewnętrznych - urządzenia nieautoryzowane. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Możliwość usuwania z listy znanych urządzeń tych nośników.
Ilość	1 szt.

VII. CZĘŚĆ NR 6

1. URUCHOMIENIE I ŚWIADCZENIE USŁUGI SAAS W POSTACI STRONY WWW ZGODNEJ Z PRZEPISAMI PRAWA, UMIESZCZONEJ W BEZPIECZNEJ CHMURZE OBLICZENIOWEJ CHRONIONEJ ROZWIĄZANIEM ANTY-DDOS, Z ZAPEWNIENIEM KOPII ZAPASOWEJ DANYCH, AKTUALIZACJĄ SYSTEMU I ZABEZPIECZEŃ, CERTYFIKATEM SSL, WSPARCIEM TECHNICZNYM I MONITORINGIEM BEZPIECZEŃSTWA

Nazwa	Minimalne wymagania dla usługi
Typ	Uruchomienie i świadczenie usługi SaaS w postaci strony www zgodnej z przepisami prawa, umieszczonej w bezpiecznej chmurze obliczeniowej chronionej rozwiązaniem Anty-DDoS, z zapewnieniem kopii zapasowej danych, aktualizacją systemu i zabezpieczeń, certyfikatem SSL, wsparciem technicznym i monitoringiem bezpieczeństwa dla Urzędu Gminy w Pępowie
Usługa chmurowa – serwis www	1. **Wymagania dla projektu graficznego usługi chmurowej – serwisu www.** 1) Projekt serwisu www musi uwzględniać zasady UI oraz UX, a także WCAG 2.1 dla całego układu serwisu www oraz rozmieszczenia elementów, jak również w kwestii zastosowanych czcionek, kontrastu elementów graficznych oraz tła itp. 2) Projekt graficzny serwisu www musi być opracowany dla różnego rodzaju wielkości ekranów, aby zapewnić responsywność. 3) Rozdzielczość dla wersji desktop szerokość wyświetlanego kontentu to 1600px, ale całość serwisu wyświetlana jest na 100% ekranu. 4) Zastosowany kontrast zgodny z wytycznymi dotyczącymi dostępności treści cyfrowych (WCAG 2.1). Współczynnik kontrastu co najmniej 4,5:1 dla zwykłego tekstu i 3:1 dla dużego tekstu (co najmniej 18 punktów) lub tekstu pogrubionego. 5) Projekt powinien zapewnić dostęp do najważniejszych informacji serwisu www, w jak najmniejszej ilości kliknięć – preferowane są max 3 kliknięcia. 6) Projekt graficzny musi być tak zaprojektowany aby była możliwość tworzenia różnych konfiguracji układu strony głównej. Realizacja tej funkcjonalności

	powinna być możliwa poprzez np. zmianę kolejności poszczególnych sekcji na stronie głównej, włączanie i wyłączanie modułów funkcjonalnych, zachowując przy tym zasady UI/UX, WCAG 2.1 oraz walory estetyczne, tak aby nie powstawały puste niewykorzystane przestrzenie na stronie głównej serwisu www. 7) Dobór kolorystyki serwisu www będzie uzgodniony z Zamawiającym. 8) Proces projektowy serwisu www uwzględniać będzie również przygotowanie wersji żałobnej, narodowej oraz świątecznej serwisu www. **2. Wymagania funkcjonalne dla usługi chmurowej – Portal www będzie posiadał minimalnie następujące funkcjonalności, które mogą być uruchomione lub nie, w zależności od potrzeb:** 1) slider aktualności, z możliwością wyłączenia przez Internautę automatycznego przesuwania się kolejnych aktualności 2) aktualności z możliwośią kategoryzacji aktualności np. Sportowe, Kulturalne itp.; integracja aktualności z modułem Galeria oraz Kalendarz wydarzeń 3) kalendarz wydarzeń zintegrowany z aktualnościami, 4) galerie zdjęć z możliwością ich przeglądania: zdjęcie następne, zdjęcie poprzednie, 5) ruchomy pasek aktualności, z możliwością wyłączenia przez Internautę, 6) slider plakatów, z możliwością wyłączenia, automatycznego przesuwania się przez Internautę, 7) system banerowy, 8) pop up, z możliwością wyłączenia przez Internautę, 9) sondę, 10) mapa serwisu odzwierciedlającą widoczne elementy struktury serwisu, 11) integracja z walidatorem Wave WCAG 2.1, 12) newsletter wraz z systemem e-mail marketing, 13) powiadomienia Web Push dla aktualności, z możliwością ich wysyłki w ramach panelu zarządzania, 14) dzień tygodnia i pogodę, 15) zadaj pytanie do, 16) katalog firm i instytucji, 17) statystyki odwiedzin zintegrowane z Google Analytics, 18) funkcja strony do druku dla każdej informacji tekstowej, dostępna poprzez ikonkę pod każdą informacją, 19) funkcja udostępnienia informacji na profilu Facebook dla każdej informacji tekstowej, dostępna poprzez ikonkę pod każdą informacją, 20) wyszukiwarka, 21) formularz kontaktowy, 22) formularz zapisu do newslettera 23) formularz zapisu do powiadmień WebPush 24) kanał RSS, 25) deklaracja dostępności, 26) wersja serwisu www w wysokim kontraście, 27) powiększanie/pomniejszanie czcionki/ zwiększanie odstępów pomiędzy znakami i wersami tekstu,

	28) informacja o miejscu w strukturze serwisu internetowego, w którym znajduje się aktualnie internauta, tzw. ścieżka dostępu, breadcrumbs **3. Wymagania dotyczące systemu CMS do zarządzania usługą chmurową - serwisem www dostępne w panelu zarządzania:** 1) panel administracyjny w polskiej wersji językowej, 2) system CMS musi posiadać mechanizm przekierowujący użytkownika na zaprojektowaną przez Dostawcę stronę informacji o błędzie (ERROR 404) w przypadku podania niewłaściwego adresu strony WWW, na której znajdzie się informacja o braku szukanego adresu oraz link do strony głównej danej strony WWW, 3) dostęp do panelu administracyjnego powinien być możliwy poprzez wejście na konkretny adres strony www, za pomocą loginu i hasła, zaszyfrowany za pomocą certyfikatu SSL, 4) system CMS dostarczony przez Dostawcę musi umożliwiać zarządzanie treścią całego serwisu internetowego bez konieczności znajomości języków programowania (do obsługi ma być wystarczająca podstawowa znajomość programów do edycji tekstu, obróbki grafiki). 5) system CMS musi obsługiwać wszystkie strony serwisu internetowego oraz wszystkie bazy, rejestry, listy etc. 6) pełne zarządzanie menu, tzn. dodawanie/usuwanie zakładek i podzakładek; możliwość stworzenia minimum 3 poziomów struktury menu, 7) tworzenie linków między zakładkami i podzakładkami, 8) budowanie hierarchii menu, w tym struktury, która pozostaje nie widoczna na stronie prezentacyjnej, 9) możliwość zmiany umiejscowienia elementów struktury menu, w tym kolejności wyświetlania oraz przenoszenia poszczególnych elementów np. podstrony jako stronę, lub odwrotnie, przyporządkowanie danej strony lub podstrony pod inny dział, stronę itd. 10) możliwość tworzenia różnych konfiguracji układu strony głównej, bazując na tym samym układzie zgodnie z załącznikiem do specyfikacji. Realizacja tej funkcjonalności powinna być możliwa poprzez np. zmianę kolejności poszczególnych sekcji strony głównej, włączanie i wyłączanie modułów funkcjonalnych, zachowując przy tym zasady UI/UX, WCAG 2.1 oraz walory estetyczne, tak aby nie powstawały puste niewykorzystane przestrzenie na stronie głównej serwisu www. 11) zarządzanie widocznością i publikacją elementów struktury, 12) możliwość podejrzenia tworzonej treści bez jej publikacji na stronie wynikowej, 13) możliwość włączenia i wyłączenia graficznej wersji żałobnej, narodowej i świątecznej serwisu, 14) łatwa, pełna edycja tekstu za pomocą WYSIWYG, w tym z możliwością: a. pogrubienia, kursywy, podkreślenia tekstu, b. wyrównania tekstu, zdjęcia, tabelki: do lewej, do środka, do prawej, równaj do prawej i lewej, c. skorzystania z wbudowanych styli: nagłówki od 1 do 6 d. skorzystania z listy wbudowanych rodzajów czcionek,

	e. określenia wielkości czcionki w danym tekście, f. określenia koloru czcionki oraz koloru tła pod tekstem, g. kopiowania, wycinania i wklejania podczas edycji treści, h. wklejania treści z edytorów tekstu np. z MS Word, i. zastosowania listy numerowanej i punktowanej, j. zastosowania wcięcia, cofnięcia wcięcia, k. cofnięcia i ponowienia operacji, l. wstawienia i edytowania linków do: pliku, zdjęcia, adresu email, strony www – z określeniem czy w tym samym oknie, czy w nowym, m. wstawienia pliku graficznego w treści za pomocą przeglądaj dysk, z możliwością ○ określenia tytułu pliku oraz opisu alternatywnego, ○ określenia pozycji zdjęcia względem tekstu (wyrównanie do lewej lub prawej, oblanie tekstem, pozycja zdjęcia względem tekstu) ○ wstawienie ramki z określeniem jej grubości, n. przełączenia się w tryb HTML, o. wstawienia filmu lub pliku audio, p. wstawienia tabeli z możliwością: ustawienia liczby kolumn i wierszy ○ określenia odległości komórek od siebie, ○ określenia zawartości komórki od jej ramki, ○ wyrównanie tabeli względem tekstu, ○ określenie obramowania tabeli, ○ szerokości i wysokości ○ kolor ramki i kolor tła, 15) dodawanie załączników, do każdej podstrony tekstowej struktury serwisu, załączony załącznik musi być być prezentowany w sposób automatyczny na stronie wynikowej (bez potrzeby ingerencji osoby redagującej), zgodnie z wymogami WCAG 2.1 tj. muszą posiadać nazwę pliku, rozmiar i typ, 16) każdy plik graficzny implementowany do zawartości serwisu www musi posiadać możliwość przy jego dodawaniu, określenia jego tytułu, opisu alternatywnego za pomocą odpowiednich pól, 17) funkcjonalność umożliwiająca zarządzanie aktualnościami: a) zarządzanie aktualnością – dodawanie nowej, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności, b) możliwość dodawania kategorii aktualności: np. dla biznesu, finansowe, itp. c) wypromowanie artykułu w sliderze, d) dodanie danego artykułu również do kalendarza wydarzeń, e) możliwość podpięcia galerii, która nie jest widoczna na stronie głównej f) możliwość umieszczenia wybranych aktualności z jednego serwisu www w innych serwisach www i odwrotnie (serwisach www powstałych w wyniku tego postępowania, zbudowanych o tę samą technologię), moduł

	moderowany – użytkownik z odpowiednimi uprawnieniami decyduje czy opublikować daną aktualność w swoim serwisie www. g) załączanie plików, w tym: ○ implementacja plików graficznych w tekście, które muszą posiadać możliwość kadrowania, obracania, powiększania i pomniejszania, tzw. ustawienia oblewania tekstem oraz obok tekstu z lewej i prawej – w celu uzyskania odpowiedniej kompozycji, ○ załączane pozostałe pliki jako załączniki – muszą być prezentowany w sposób automatyczny na stronie wynikowej (bez potrzeby ingerencji osoby redagującej), zgodnie z wymogami WCAG 2.1 tj. muszą posiadać nazwę pliku, rozmiar i typ, 18. funkcjonalność umożliwiająca zrządzanie galerią zdjęć: a. zarządzanie galerią – dodawanie nowej, edycja i usuwanie, ukrywanie, pokazywanie, zmianę kolejności, b. dodawanie zdjęć potokowo(czyli dużej ilości plików jednorazowo) za pomocą technologii Drag& Drop, c. dodawanie zdjęć potokowo za pomocą opcji przeglądaj z dysku, d. dodawanie pojedyncze zdjęć, e. określenie nazwy dodawanych zdjęć lub nadanie im nazwy z danej galerii, f. automatyczną kompresję plików o dużej pojemności i dostosowywanie ich do optymalnych cech (rozmiar w px, pojemność w MB), w celu ich poprawnej publikacji ze względu na wysokość ekranu i szybkości ładowania na stronie www, g. przeglądanie zdjęć za pomocą wbudowanej przeglądarki, prezentującej zdjęcia na warstwie, umożliwiającej przechodzenie do następnego zdjęcia oraz poprzedniego, a także zamykanie okna. 19. funkcjonalność umożliwiająca zrządzanie kalendarzem wydarzeń: a. zarządzanie wydarzeniem – dodawanie nowego, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności, b. ustawienie nazwy wydarzenia, c. ustawienie daty wydarzenia, d. ustawienie od kiedy do kiedy dane wydarzenie ma trwać, e. ustawienie od kiedy do kiedy dane wydarzenie ma być widoczne w kalendarzu, 20. funkcjonalność umożliwiająca zrządzanie ruchomym paskiem informacyjnym: a. zarządzanie – dodawanie nowej informacji, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności, b. ustawienie tytułu informacji, c. ustawienie daty informacji, d. zlinkowanie do strony zewnętrznej lub elementu struktury serwisu www, e. możliwość przypisania galerii,

	21. funkcjonalność umożliwiająca zrządzanie banerami w określonych miejscach serwisu www np. polecamy, na skróty, zdjęcia w top, zdjęcie dla modułu statystycznego: a. zarządzanie banerami - dodawanie nowego, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności, b. tworzenie pop-up na warstwie, c. możliwość linkowania do stron zewnętrznych oraz podstron serwisu, d. slider plakatów – funkcjonalność umożliwiająca prezentację plików w formacie pionowym, 22. funkcjonalność umożliwiająca zrządzanie sondą: a. zarządzanie sondą - dodawanie nowego, edycja, usuwanie, ukrywanie, pokazywanie, zmianę kolejności, b. tworzenie pytania, c. tworzenie nagłówka sondy, d. ustawienia opcji głosowania: wielokrotne, jednokrotne, e. widoczność sondy od ..do, f. widoczność wyników głosowania tak/nie, 23. funkcjonalność umożliwiająca zarządzanie – zadaj pytanie: a. Zarządzanie listą osób/stanowisk do których można zadać pytanie poprzez formularz „Zadaj pytanie” : niezbędne pola: Imię i Nazwisko lub Stanowisko, adres email, widoczność, pozycja – kolejność osób na liście, usuń/edytuj, dodaj; 24. funkcjonalność umożliwiająca zarządzanie – katalogiem firm i instytucji a. Dodawanie kategorii w biznesie lub rodzaju instytucji np. Apteki, Lekarze, Hotele itp. b. Możliwość dodawania wpisu do katalogu przez redaktora lub internautę, z podaniem nazwy i danych adresowych danego podmiotu, wyborem branży, krótkim opisem i zdjęciem, adres www, email kontaktowy, wymagane podanie adresu email i telefonu dla dodającego internauty, c. Moduł moderowany – redaktor weryfikuje i decyduje które wpisy będą wyświetlane i w jakiej formie i kategorii. 25. newsletter wraz z systemem e-mail marketing, z możliwością: a. skonfigurowania konta do wysyłki newsletterów bez użycia zewnętrznego programu pocztowego, b. tworzenia wiadomości do wysłania za pomocą newslettera, w tym z załącznikami, z automatycznym linkiem do rezygnacji z prenumeraty oraz innym zaprojektowanym tekstem, c. tworzenie i zarządzanie szablonów wiadomości w tym co najmniej: ○ wiadomości usunięcia konta, ○ wiadomość powitalna po aktywacji, ○ wiadomość aktywacji konta, d. tworzenia kopii roboczych wiadomości,

	e. tworzenia i zarządzania grupami mailingowymi, f. przechowywania wiadomości do wysyłki w skrzynce nadawczej z następującymi funkcjami: o o w przypadku zamknięcia skrzynki nadawczej w trakcie wysyłania np. wylogowanie się, brak prądu – wysyłka zostaje przerwana, a nie anulowana, o ponowne otwarcie skrzynki nadawczej kontynuuje wysyłkę od momentu w jakim została przerwana, o w trakcie wysyłki mailingu można zatrzymać proces, o podczas wysyłki mailingu, na bieżąco podawana jest informacja o ilości wysyłanych wiadomości, g. przechowywania wysłanych wiadomości w elementach wysłanych, w tym z informacjami : o do ilu adresatów wysłano mailing, o o ilości kliknięć w odnośniki (linki) w wiadomości- wartość liczbowa, o o ilości kliknięć w odnośniki (linki) w wiadomości- wartość procentowa, o o ilości otwarć (odczytu) wiadomości – wartość liczbowa, o o ilości otwarć (odczytu) wiadomości – wartość procentowa, o o dacie wysyłki, h. przetestowania poprawności wysyłki oraz struktury wysyłanej wiadomości na określone adresy email, i. zarządzania adresami email, w tym z możliwością o usuwania i dodawania adresów ręcznie, o importu adresów email z pliku csv, w tym z możliwością: ✓ automatycznego aktywowania importowanych adresów email, ✓ pominięcia adresów email, które występują w innych grupach mailingowych, o podglądem statusu adresu email – czy jest aktywny czy nieaktywny, o usuwaniem z bazy zaznaczonych adresów, o subskrybowaniem zaznaczonych adresów, o wypisaniem zaznaczonych adresów, o przypisaniem i dodaniem zaznaczonych adresów do grup, o aktywowanie i deaktywowanie zaznaczonych adresów, o uzyskania informacji: ✓ adresie email, ✓ dacie dodanie adresu do bazy mailingowej, ✓ o adresie IP skąd nastąpiło dodanie adresu, ✓ ile wysłano wiadomości do tego adresu, ✓ ile było kliknięć w odnośniki w treści wiadomości przez użytkownika tego adresu,

	✓ ile było otwarć wiadomości (odczytu) przez użytkownika adresu email ✓ do jakiej grupy przypisany jest adres email, ✓ status adresu: aktywny, nieaktywny, wypisany, niewypisany. j. k. przeszukiwania skrzynki po wysłaniu mailingu, w celu zidentyfikowania i usunięcia emaili, generujących tzw. odbicia – czyli adresów email, do których dana wiadomość nie dotarła, l. konfigurowania działania systemu newsletter w przypadku odbić twardych oraz miękkich, w tym co najmniej: ○ w przypadku odbić twardych – konfiguracja komunikatów dotyczących przyczyny odbicia, zgodnie z systematyką komunikatów błędów poczty email; np. account not found, host not found, ○ w przypadku odbić miękkich: ✓ konfiguracja komunikatów dotyczących przyczyny odbicia, zgodnie z systematyką komunikatów błędów poczty email; np. skrzynka przepełniona itp. ✓ konfiguracja ilości odbić miękkich, które przekształcą się w odbicie twarde: ile razy skrzynka musi odbić wiadomość ✓ konfiguracja ilość dni, w których odbicie miękkie jest ignorowane: przez ile dni wiadomość jest odrzucana, 26. funkcjonalność zarządzania użytkownikami systemu: a. lista użytkowników, b. dodawanie i zarządzanie użytkownikami c. nadawanie uprawnień do poszczególnych modułów oraz funkcjonalności dla utworzonych grup, d. funkcjonalność tworzenia i zarządzania grupami użytkowników np. administratorzy, redaktorzy – wraz z przydzieleniem ich dostępu do określonych modułów, funkcjonalności, e. możliwość odblokowywania zablokowanych użytkowników z powodu błędnego logowania, 27. funkcjonalność wymuszenia zmiany hasła logowania się do panelu zarządzania, w tym co najmniej: a. możliwość określenia ilości dni ważności hasła b. możliwość określenia ilości tygodni ważności hasła c. możliwość określenia ilości miesięcy ważności hasła 28. funkcjonalność logowania dwuetapowego do panelu zarządzania, w tym co najmniej: a. zastosowanie mechanizmu poprzez Google Authenticator lub Microsoft Authenticator lub inny równoważną aplikację

	b. uwierzytelnianie za pomocą klucza w aplikacji uwierzytelniającej 29. funkcjonalność integracji z kontem Google Analytics w celu uzyskania szczegółowych statystyk odwiedzalności serwisu, w tym co najmniej: a. graficzne w formie wykresu i liczbowe, przedstawienie statystyk odwiedzalności, w podziale na godziny, dni, tygodnie oraz niestandardowy, w tym zakres określonych dat, b. publikacja informacji o liczbie: sesji, użytkownikach, nowych użytkownikach, odsłonach, średnim czasie trwania sesji, strony/sesję, 30. funkcjonalność SEO – w celu określenia podstawowych danych serwisu, podlegających indeksowaniu przez wyszukiwarki internetowe, umożliwiająca co najmniej: a. określenie pola Title (tytuł), b. określenie pola Descryption (Opis), c. określenie keywords (słów kluczowych), 31. funkcjonalność konfiguracji kont email przeznaczonych do obsługi np. formularza kontaktowego, newslettera, 32. funkcjonalność tworzenia, udostępnienia i zarządzania deklaracją dostępności zgodnej ze wzorem opublikowanym przez właściwego Ministra, zgodnie z wymogami Ustawy o dostępności cyfrowej z dnia 4 kwietnia 2019 roku. 33. funkcjonalność generowania raportów: a. Liczba subskrybentów usługi newsletter oraz zarządzanie adresami, import list mailingowych b. Zajętości miejsca na serwerze oraz ilość odwiedzin/wizyt w danym miesiącu c. Liczba otwarć i kliknięć dla wysłanych newsletterów 34. funkcjonalność konfiguracji WEB APP Manifest umożliwiająca co najmniej: a. Określenie pełnej nazwy strony b. Skróconej nazwy strony c. Krótkiego opisu strony 35. funkcjonalność wbudowanego w wysiwyg Asystenta Sztucznej Inteligencji AI wspierający proces redaktorski umożliwiający co najmniej określenie: a. Ilość znaków danej informacji/artykułu b. Określenie stopnia kreatywności i konkretności w tworzonym modelu informacji/artykułu od 0,1 do 1,0 c. wpisanie klucza API z wykupionej usługi 36. funkcjonalność archiwum dla aktualności, wydarzeń, stron i podstron oraz załączników: a. możliwość aktywacji lub dezaktywacji archiwum, b. możliwość usuwania elementów z archiwum po określonej liczbie dni, c. możliwość przywrócenia elementu z archiwum, d. archiwum stron i podstron – umożliwia podejrzenie struktury nadrzędnej dla zarchiwizowanego elementu.

	4. Pozostałe wymagania dla usługi chmurowej - serwisu www. 1) Wykonana usługa chmurowa – serwis www powinien spełniać wymagania obowiązujących przepisów prawa. 2) Usługa chmurowa powinna posiadać aktywną ochronę AntyDDos o następujących właściwościach: a. Ochrona przed atakami wolumetrycznymi w warstwie 3 i 4 modelu OSI, b. Aktywny monitoring, reagowanie na ataki, c. Zabezpieczenie punktu styku z siecią publiczną przed atakami o wolumenie do 80Gbps, d. Minimalny lub równoważny zakres rodzajów odpieranych ataków: o ICMP - smurf attack o CMP - ping flood o LAND o Christmas tree o TCP SYN Flood o UDP flood o NTP reflected/amplification attack o DNS reflected/amplification attack o CLDAP Amplification / Reflection attack o CHARGEN Amplification / Reflection attack o L2TP Amplification / Reflection attack o MSSQL Amplification / Reflection attack o NetBIOS Amplification / Reflection attack o RCPBIND Amplification / Reflection attack o RIPv1 Amplification / Reflection attack o SNMP Amplification / Reflection attack o mDNS Amplification / Reflection attack o SSDP Amplification / Reflection attack o Memcached Amplification / Reflection attack o UDP/IP Fragments o Generic UDP Reflection o QOTD Reflection o DNS Query Flood o Invalid packets - IP checksum o Invalid packets - IP NULL o Invalid packets - TCP flags o Invalid packets - Bad UDP Payload length o TCP Fragments o TCP RST Flood e. Minimalny lub równoważny zakres metod obrony/blokowania: blokowanie/czasowe zawieszanie źródłowych adresów IP o blokowanie wybranych pakietów o kombinacja blokowania adresów IP bazująca na nagłówkach pakietów oraz progach ilościowych o obsługa BGP Flowspec

	○ obsługa BGP Blackhole f. Minimalny lub równoważny zakres mechanizmów używanych w trakcie obrony: ○ SYN Filter ○ Token Bucket Filter ○ WHITE/BLACK LIST ○ DROP ○ Invalid Packet Filter ○ Adaptive Filter ○ GeoFilter ○ Automatycznie aktualizowana black list 3) Usługa chmurowa musi: a. być realizowana w minimum dwóch różnych lokalizacjach na obszarze UE, w kwestii wykorzystywanych zasobów serwerowych dla świadczenia usługi chmurowej, w tym również dla zapewnienia backupów danych, b. być realizowana w oparciu o aktualny Certyfikat ISO 27001 lub inny równoważny w aspekcie potwierdzenia stosowania systemu zarządzania bezpieczeństwem informacji dla usługi chmurowej – należy przedstawić kopie certyfikatu, c. być zgodna z systemem zarządzania bezpieczeństwem dla wymagań SCCO1 i lub SCCO2 określonymi w Standardach Cyberbezpieczeństwa Chmur Obliczeniowych – należy załączyć oświadczenie o zgodności, d. być świadczona w Centrum Przetwarzania Danych, które spełnia wymagania normy PN-EN 50600 minimum klasy 3 lub ANSI/TIA-942 minimum Tier III, lub innego normatywu odpowiedniego i powszechnie uznanego do oceny CPD – należy przedstawić minimum kopię certyfikatu. 4) Serwis internetowy powinien być przygotowany w wersji responsywnej (automatycznie dopasowującej się rozdzielczości urządzeń na których jest przeglądana, a także do różnych przeglądarek internetowych). 5) Serwis internetowy powinien być przygotowany w technologii umożliwiającej korzystanie ze strony internetowej na urządzeniach mobilnych w podobny sposób, jak działa mobilna aplikacja natywna. Serwis www musi posiadać możliwość „zainstalowania” na urządzeniach mobilnych poprzez dodanie ikonki na ekran urządzenia mobilnego, po tej czynności w celu przeglądania treści serwisu, wystarczy kliknąć na ikonkę strony www, a strona będzie działała jak mobilna aplikacja mobilna- treści powinny być częściowo dostępne nawet, bez połączenia z Internetem- technologia Progressive Web Apps (PWA) lub równoważna. 6) Technologia wykonania powinna pozwalać na rozbudowę serwisu www oraz na podłączenie dodatkowych funkcjonalności w przyszłości. 7) Zarówno serwis www, jak i system CMS powinny być obsługiwane przez najpopularniejsze i najbardziej aktualne przeglądarki: Edge, Mozilla Firefox, Google Chrome, Opera.

	8) Wymagane jest zastosowanie technologii PHP, AJAX, PWA bądź innych technologii o porównywalnych możliwościach. 9) Narzędzia do obsługi serwisu www muszą spełniać zalecenia ATAG i być dostępne dla użytkowników niepełnosprawnych, a w szczególności: a. Serwis internetowy powinien dać się obsłużyć przy użyciu klawiatury. b. Serwis internetowy nie może być zbudowany na bazie tabel, traktowanych jako element konstrukcji layoutu. c. Wszystkie elementy graficzne muszą mieć możliwość ustawienia tekstu alternatywnego przez redaktora. d. Serwis internetowy powinien oferować dostęp do wszystkich informacji przy wyłączonej obsłudze Java Script. e. Wszystkie formularze w serwisie muszą być zgodne ze standardami i przetestowane pod kątem dostępności dla osób niepełnosprawnych. 10) Każdy widok serwisu www musi mieć przez cały czas widoczny link/element graficzny umożliwiający powrót do strony głównej. 11) Zamawiający dopuszcza ze względów cyberbezpieczeństwa danych tylko dedykowane dla jednostek administracji publicznej, autorskie rozwiązanie CMS, czyli CMS nie może być oparty o rozwiązanie Open Source. a. Serwis internetowy BIP powinien oferować dostęp do wszystkich informacji przy wyłączonej obsłudze Java Script. b. Wszystkie formularze w serwisie muszą być zgodne ze standardami i przetestowane pod kątem dostępności dla osób niepełnosprawnych. 12) Każdy layout strony musi mieć przez cały czas widoczny link umożliwiający powrót do strony głównej z każdego miejsca na stronie WWW i odsyłacz umożliwiający powrót na początek strony. 13) Zamawiający dopuszcza ze względów bezpieczeństwa danych tylko dedykowane dla jednostek administracji publicznej, autorskie rozwiązanie CMS.
Wymagania dodatkowe	Zamawiający wymaga dodatkowo: 1) wdrożenia systemu CMS który będzie posiadał specyficzne funkcjonalności zgodnie z opisem przedmiotu zamówienia 2) Przedstawienia min. 1 zgodnego z wymaganiami projektu graficznego dla serwisu www. 3) Świadczenia usług chmurowych na okres do 30.06.2026 r. nielimitowanego transferu danych, backupu danych, zabezpieczenia serwera, utrzymania usługi, 4) zapewnienia min. 5 GB przestrzeni na serwerach dla każdej usługi chmurowej, 5) przeprowadzenia szkolenia online z zakresu obsługi CMS dla usługi chmurowej a także modułów funkcjonalnych, 6) udzielenia gwarancji na przedmiot zamówienia w okresie 24 miesięcy, 7) do usuwania wad i błędów, w tym aktualizacji pod kątem bezpieczeństwa i zgodności z przeglądarkami (m. in. Firefox, Edge, Safari, Opera, Chrome), dokonywania napraw, usuwanie wszelkich usterek funkcjonalnych i technicznych w okresie gwarancji, 8) udzielenia i świadczenia usługi aktualizacji systemu CMS, a także dostosowywania funkcjonalności usługi chmurowej - strony www i elementów technicznych systemu CMS w okresie gwarancji do zmieniających się przepisów prawa,

	9) udzielania bezpłatnych porad telefonicznych osobom wskazanych przez Zamawiającego w zakresie obsługi CMS (porady udzielane mają być w dni robocze, tj. od poniedziałku do piątku, w godz. 8.00 - 16.00) przez okres trwania gwarancji.
Ilość	1 szt.