OCiZK.271.1.2025.KJ

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego pn.:

Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd" w Gminie Pyrzyce w ramach: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (DERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd"

Spis treści

I ZAMAWIAJĄCY

GMINA PYRZYCE, ul. PLAC RATUSZOWY 1, 74-200 PYRZYCE, tel.: (91) 3970310,

NIP: 853-145-69-90, REGON: 811 685 711

Niniejszy dokument określa minimalne wymagania dla zamówienia z zakresu cyberbezpieczeństwa w ramach realizacji projektu „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".

Postępowanie prowadzone jest zgodnie z postanowieniami ustawy prawo zamówień publicznych z dnia 11 września 2019 r. (dz.u. z 2023 r. poz. 1605) oraz aktów wykonawczych wydanych na jej podstawie.

Niniejsze postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, w którym w odpowiedzi na ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani Wykonawcy, a następnie Zamawiający wybiera najkorzystniejszą ofertę bez przeprowadzenia negocjacji (art. 275 pkt 1 ustawy Pzp). Zamawiający nie przewiduje możliwości wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji (art. 275 pkt 2 ustawy Pzp).

Zamawiający w okresie 3 lat od dnia udzielenia zamówienia podstawowego, dotychczasowemu wykonawcy nie przewiduje udzielenia zamówienia polegającego na powtórzeniu podobnych usług.
Zamawiający nie dopuszcza składania ofert wariantowych.
Zamawiający nie przewiduje wymagań wskazanych w art. 96 ust. 2 pkt 2 ustawy Pzp.
Zamawiający nie przewiduje wymagań wskazanych w art. 94 ustawy Pzp.
Zamawiający nie przewiduje zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.
Zamawiający nie wymaga przeprowadzenia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy Pzp.
Zamawiający nie przewiduje rozliczenia między Zamawiającym a Wykonawcą w walutach obcych.

Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

Zamawiający nie wymaga obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań zgodnie z art. 60 i art. 121 ustawy Pzp.

Zamawiający nie przewiduje zawarcia umowy ramowej

Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230 ustawy Pzp.

Zamawiający nie stawia wymogu lub możliwości złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93 ustawy Pzp.

Wykonawca jest związany ofertą do dnia 16.05.....2025 roku. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa w pkt 15.1 SWZ, Zamawiający przed upływem terminu związania ofertą, zwróci się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni. Przedłużenie terminu związania ofertą, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

Zamawiający nie wymaga wniesienia wadium ani zabezpieczenia należytego wykonania umowy.

II Definicje

Zamawiający dokonał opisu przedmiotu z wykorzystaniem następujących definicji:

Lp.	Termin	Definicje
1.	**OPZ**	Opis przedmiotu zamówienia
2.	**Umowa**	Należy przez to rozumieć umowę zawartą między zamawiającym a jednym lub większą liczbą wykonawców, której celem jest ustalenie warunków dotyczących zamówień, jakie mogą zostać udzielone w danym okresie, w szczególności cen i, jeżeli zachodzi taka potrzeba, przewidywanych ilości
3.	**Zamawiający**	Należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, obowiązaną na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych do jej stosowania.
4.	**Wykonawca**	należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która oferuje na rynku wykonanie robót budowlanych lub obiektu budowlanego, dostawę produktów lub świadczenie usług lub ubiega się o udzielenie zamówienia, złożyła ofertę lub zawarła umowę w sprawie zamówienia publicznego.

III Wartość zamówienia

1. Szacunkowa wartość zamówienia nie przekracza wyrażoną w złotych równowartość kwoty określonej w przepisach wydanych na podstawie ustawy prawo zamówień publicznych z dnia 11 września 2019 r. (dz.u. z 2023 r. poz. 1605).

IV Tajemnica przedsiębiorstwa

1. Zamawiający nie ujawnia informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (j.t. Dz. U. z 2022 r. poz. 1233 ze zm.), jeżeli Wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
2. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o: 1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte; 2) cenach lub kosztach zawartych w ofertach.
3. Zastrzeżenie informacji może dotyczyć nie tylko oferty, ale i innych dokumentów czy informacji składanych przez wykonawcę w postępowaniu. Dla skuteczności dokonanego zastrzeżenia należy wypełnić następujące warunki:
    - Informacje stanowiące tajemnicę przedsiębiorstwa w całości lub części danego dokumentu powinny być złożone w oddzielnej części oferty (przykładowo w odrębnym folderze, dokumencie elektronicznym) i jednoznacznie oznaczone w nazwie pliku, dokumencie czy jego fragmencie.
    - Przykładowo w nazwie pliku oznaczenie: „Załącznik stanowiący tajemnicę przedsiębiorstwa" W przypadku treści dokumentu czy informacji oznaczenie fragmentu oznaczonego tajemnicą przedsiębiorstwa może zostać dokonane przykładowo poprzez oznaczenie kolorem, wskazanie punktów czy rozdziałów, dokumentu, w którym zawarte są informacje stanowiące tajemnicę przedsiębiorstwa.
4. Wykonawca ma obowiązek równocześnie z dokonanym zastrzeżeniem wykazać, że zastrzeżone informacje stanowią tajemnice przedsiębiorstwa. Wymagania w tym względzie normuje definicja tajemnicy przedsiębiorstwa: Ustawa o zwalczaniu nieuczciwej konkurencji Art. 11. 2. "Przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w

szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności."

V Opis przedmiotu zamówienia

Część 1

1. **Serwer – 1 sztuki.**

Parametr	Wymagane minimalne wymagania techniczne
Obudowa	• Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.

RAM	• Minimum 256GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	• Demand Scrubbing, • Patrol Scrubbing, • Permanent Fault Detection (PFD)
Gniazda PCI	• Min. dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • Dodatkowa karta SAS (4x mini SAS-HD, 12Gb/s, SAS, PCIe) • Dodatkowa karta Dual Port (2x RJ-45, 10Gb/s, 10GBase-T, PCIe)
Dyski twarde	• Zainstalowane ○ 2x dysk SSD SATA o pojemności min. 480GB, 12Gb, 2,5" Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Kontroler RAID	• Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10
Wbudowane porty	• 4x USB, w tym min. 1 porty USB 3.0 • 2x port VGA (jeden na panelu przednim) • Możliwość rozbudowy o Serial Port
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	• Redundantne, Hot-Plug
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium
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 dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • 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. 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 połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ 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; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ 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 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: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is" do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby

	instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ 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. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • 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	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.
	• 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 od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, 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 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 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

2. **Serwer – 1 sztuki.**

Parametr	Minimalne wymagania techniczne
Obudowa	• Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz,

	dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	• Minimum 256GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	• Demand Scrubbing, • Patrol Scrubbing, • Permanent Fault Detection (PFD)
Gniazda PCI	• Min. dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • Dodatkowa karta Dual Port (2x RJ-45, 10Gb/s, 10GBase-T, PCIe)
Dyski twarde	• Zainstalowane ○ 2x dysk SSD SATA o pojemności min. 480GB, 12Gb, 2,5" Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Kontroler RAID	• Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10
Wbudowane porty	• 4x USB, w tym min. 1 porty USB 3.0 • 2x port VGA (jeden na panelu przednim) • Możliwość rozbudowy o Serial Port
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	• Redundantne, Hot-Plug
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium

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 dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • 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. 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 połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ 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; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ 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 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: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is" do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby

	instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ 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. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • 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	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.
	• 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 od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, 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 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 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

3. Macierz dyskowa – 1 sztuka.

Element konfiguracji/cecha/funkcjonalność	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U oraz umożliwiać montaż min. 12 dysków 3.5"
Przestrzeń dyskowa	Zainstalowane: 6x dysk SAS o pojemności min. 2.4TB, Hot-Plug 6x dysk NLSAS o pojemności min. 16TB, 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 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 iSCSI 25Gb (4 porty na kontroler),
Kable/wkładki	4x kabel DAC 25GbE SFP28-SFP28 min. 5m
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	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do

macierzy	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, RHEL, SLES, Vmware, Citrix. 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. Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold.
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)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.

	Deklaracja zgodności CE.
Warunki gwarancji	5 lat gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. 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. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

4. Serwer do wykonywania kopii zapasowych – 1 sztuka.

Komponent	Minimalne wymagania
Obudowa i pojemność	Wysokość maksymalnie 1U do instalacji w szafie Rack. Co najmniej 9 slotów przeznaczonych na zestaw taśm.
Połączenie	Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów.
Napęd	Wyposażony w co najmniej 1 sztukę napędu SAS LTO8. W komplecie:

	• kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m • 10x taśma LTO8 WORM • Oznaczenia dla taśm LTO8, numery: 1-200 • Oznaczenia dla taśm LTO8 WORM, numery: 1-200 • Taśma czyszcząca
Gwarancja	5 lat gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. 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. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

5. Zarządzane urządzenia sieciowe z obsługą VLAN – 2 sztuki.

Lp.	Minimalne wymagania Zamawiającego	
I.	**CECHY ZARZĄDZANIA**	
1.	Typ przełącznika	Zarządzany
2.	Przełącznik wielowarstwowy	L2/L3
3.	Obsługa jakość serwisu (QoS)	Tak
4.	Zarządzany w chmurze	Tak
5.	Zarządzanie przez stronę www	Tak
6.	Inspekcja ARP	Tak
7.	Konfigurowanie ustawień lokalizacji (CLI)	Tak
8.	Obsługa MIB	Tak
II.	**OCHRONA**	
9.	Funkcje DHCP	DHCP relay, DHCPv6 client
10.	Lista kontrolna dostępu (ACL)	Tak

VII.	**Monitoring**
1.	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
2.	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
3.	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.
4.	System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
5.	System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
6.	System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
7.	System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
8.	System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
9.	System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów

10.	System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
11.	System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
12.	System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
13.	System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
14.	System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
15.	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.
16.	System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
17.	System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4
VIII.	**Raportowanie**

1.	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
2.	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.
3.	System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
4.	System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
5.	System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
6.	System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
7.	System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
8.	System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
9.	System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych

10.	System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
11.	System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
12.	System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
13.	System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
14.	System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
15.	System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
16.	System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
17.	System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

Część 2

1. **Oprogramowanie przeciwdziałające wyciekowi danych.**

Oprogramowanie przeciwdziałające wyciekowi danych

Oprogramowanie na licencji wieczystej z wsparciem na okres nieprzekraczający daty 30.06.2026 r. na minimum 145 stanowisk.

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania:

    kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.
15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
    a. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
    b. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.

17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
    a. logowanie oraz wylogowanie użytkownika,
    b. włączenie oraz wyłączenie stacji roboczej,
    c. blokada oraz odblokowanie stacji roboczej,
    d. przejście w stan bezczynności stacji roboczej.
19. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
20. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
21. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
22. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
23. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
24. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
25. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.
26. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
27. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
28. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
29. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania.

30. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.
31. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
32. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
    a. aplikacje, z której zostały utworzone,
    b. lokalizację,
    c. adres URL,
    d. format pliku,
    e. zawartość pliku.
33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
34. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
    a. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
    b. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
    c. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
    d. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
    e. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
    f. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
    g. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
        - Dropbox,
        - Google Drive,
        - SharePoint,
        - OneDrive Business,
        - OneDrive Personal.
    h. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
    i. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
    j. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,

k. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,

35. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
36. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
37. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
38. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
39. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e- mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
40. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
41. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
42. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
43. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
44. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
45. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
    a. numery kart kredytowych,
    b. numer PESEL,
    c. numer polskiego dowodu osobistego,
    d. polski numer paszportu,
    e. wyrażenia regularne,
    f. określone ciągi znaków,
    g. numer IBAN.
46. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
47. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).

48. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
49. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e- mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy").
50. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
51. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
52. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM.
53. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
54. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:
    a. audyt i logowanie wiadomości e-mail,
    b. audyt i logowanie operacji na plikach,
    c. wprowadzanie polityk zabezpieczeń do wiadomości e-mail.
55. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).
56. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
57. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
    a. Bezpieczeństwo danych:
        - Przegląd informacji o incydentach bezpieczeństwa.
        - Przegląd danych przychodzących.
        - Przegląd danych wychodzących.
        - Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.
        - Podłączane/odłączane urządzenia przenośne.
    b. Produktywność:
        - Przegląd informacji na temat produktywności użytkowników.
        - Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
        - Trendy.
    c. Eksploatacja sprzętu:
        - Przegląd informacji na temat eksploatacji sprzętu komputerowego.
        - Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
        - Eksploatacja drukarek.
        - Eksploatacji sieci.

2. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.

3. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.

4. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt.:

- plików przenoszonych na nośniki USB i inne urządzenia przenośne,
- plików przesłanych za pomocą wiadomości e-mail,
- plików przesłanych za pomocą poczty webowej,
- plików przesłanych do Internetu,
- plików wysłanych za pomocą komunikatorów,
- plików przesłanych na dyski chmurowe,
- analiza sposobu korzystania z aplikacji,
- analiza korzystania z Internetu,
- analiza wykorzystania porali do poszukiwania pracy.

Część 3

1. Wdrożenie systemów teleinformatycznych.

Wdrożenia klastra serwerów

Krok 1: Planowanie i Przygotowanie

- Określenie wymagań dotyczących infrastruktury, w tym sprzętu, sieci i przechowywania.
- Wybranie serwerów, które zostaną użyte jako węzły klastra. Upewnij się, że są one zgodne z wymaganiami wybranego oprogramowania.
- Skonfigurowanie łącza sieciowego i przestrzeni dyskowej, aby zapewnić odpowiednią przepustowość i pojemność.
- Zainstalowanie systemu operacyjnego na każdym węźle klastra.

Krok 2: Instalacja roli oprogramowania do wirtualizacji

- Instalacja odpowiedniej roli za pomocą menedżera serwerów lub PowerShell.
- Konfiguracja ustawień sieciowych i przechowywania na węzłach klastra, tak aby były zgodne z wymaganiami projektu.

Krok 3: Konfiguracja klastra

- Uruchomienie kreatora konfiguracji klastra w menedżerze serwerów na jednym z węzłów.
- Dodanie pozostałych węzłów klastra do konfiguracji.
- Konfiguracja ustawień klastra, takie jak nazwa klastra, adresy IP i konfiguracja przechowywania współdzielonego.

Krok 4: Konfiguracja wysokiej dostępności klastra

- Włączenie funkcji wysokiej dostępności dla maszyn wirtualnych na klastrze.
- Konfiguracja ustawień zapasowych dla klastra, aby zapewnić ochronę przed awariami węzłów.

Krok 5: Tworzenie i Zarządzanie Maszynami Wirtualnymi

- Utworzenie nowych maszyn wirtualnych na klastrze z wykorzystaniem oprogramowania do wirtualizacji.
- Konfiguracja ustawień maszyn wirtualnych, takich jak liczba procesorów, ilość pamięci i przypisywanie zasobów sieciowych.
- Zarządzanie maszynami wirtualnymi, monitorowanie ich wydajności i wykonywanie niezbędnych operacji konserwacyjnych jest kluczowe w zapewnieniu prawidłowo funkcjonującego środowiska wirtualnego uruchomionego w klastrze.

Krok 6: Testowanie i Monitorowanie

- Testowanie działania klastra, w tym jego zdolność do migracji wirtualnej i przywracania po awariach.
- Konfiguracja narzędzi monitorujących, w celu śledzenia wydajności i dostępności klastra oraz maszyn wirtualnych.
- Regularnie przeglądanie logów i raportów, w celu szybkiego reagowania na ewentualne problemy.

2. Wirtualizacja serwerów i segmentacja sieci.

Przedmiotem zamówienia jest wykonanie kompleksowej wirtualizacji serwerów w celu utworzenia klastra dla maksymalnie 10 usług w infrastrukturze Zamawiającego. Projekt obejmuje przygotowanie, instalację, konfigurację i monitorowanie środowiska wirtualnego.

1. **Sprawdzenie wymagań systemowych**:
   - Upewnij się, że serwery, na których chcesz utworzyć klaster, spełniają minimalne wymagania systemowe dla Hyper-V.

1. Minimalne wymagania:

a. Wymagania sprzętowe:

b. Procesor: 64-bitowy procesor z obsługą wirtualizacji (Intel VT lub AMD-V).

c. Pamięć RAM: Co najmniej 4 GB, chociaż zalecane są większe ilości, szczególnie jeśli planujesz uruchamiać wiele wirtualnych maszyn.

d. Dysk twardy: Przestrzeń dyskowa wystarczająca do zainstalowania systemu operacyjnego i aplikacji, oraz dodatkowo miejsce na przechowywanie plików wirtualnych maszyn.

e. Karta sieciowa: Karta sieciowa wspierająca TCP/IP, najlepiej z obsługą Gigabit Ethernet.

2. Wymagania systemowe:

a. Wersja systemu operacyjnego: Hyper-V jest dostępny w wybranych edycjach systemu Windows Server, takich jak Windows Server Standard, Datacenter, Essentials, i innych.

b. Aktualizacje: Zalecane jest regularne stosowanie aktualizacji systemu operacyjnego i aktualizacji zabezpieczeń dla bezpieczeństwa i wydajności.

c. Wymagania dotyczące wirtualizacji:

d. Włączone funkcje wirtualizacji w BIOS/UEFI komputera.

e. Wsparcie dla Second Level Address Translation (SLAT), jeśli chcesz uzyskać pełną wydajność wirtualizacji w systemie Windows 8 lub nowszym.

3. Wymagania dodatkowe:

a. Jeśli planujesz tworzyć klastry HA, wymagane jest co najmniej dwa fizyczne serwery z odpowiednim sprzętem i siecią.
   - Upewnij się, że posiadają one odpowiednie zasoby sprzętowe, takie jak procesory, pamięć RAM i przestrzeń dyskowa.

2. **Instalacja systemu operacyjnego**:
   - Zainstalowanie na serwerach odpowiedniej wersji systemu operacyjnego umożliwiającego wirtualizację.
3. **Włączenie funkcji Hyper-V**:
   - Włączenie funkcji wirtualizacji w BIOS/UEFI oraz instalacja i konfiguracja odpowiednich ról i funkcji do zarządzania wirtualizacją.
4. **Konfiguracja sieci**:
   - Skonfigurowanie sieci wirtualnych oraz interfejsów sieciowych do zapewnienia komunikacji między wirtualnymi maszynami, a także z siecią lokalną i zewnętrzną.
5. **Przygotowanie pamięci masowej**:

- Konfiguracja przestrzeni dyskowej na każdym z serwerów w celu przechowywania danych wirtualnych maszyn i ich plików konfiguracyjnych. Możliwe wykorzystanie wspólnej przestrzeni dyskowej typu Sieć Przestrzeni Dyskowej (SMB) do efektywniejszego zarządzania danymi.

6. **Konfiguracja klastra**:
   - Utworzenie klastra wirtualizacji poprzez dodanie serwerów i skonfigurowanie ustawień klastra, w tym nazwy, adresu IP, oraz trybu zasilania.
7. **Konfiguracja magistrali klastra**:
   - Umożliwienie komunikacji między serwerami poprzez konfigurację magistrali klastra oraz lokalizację Quorum w odrębnej lokalizacji SMB.
8. **Wdrożenie wirtualnych maszyn**:
   - Instalacja i konfiguracja wirtualnych maszyn, w tym zapewnienie odpowiedniej konfiguracji dla migracji w przypadku awarii.
9. **Testowanie i monitorowanie**:
   - Przeprowadzenie testów funkcji HA i migracji wirtualnych maszyn, monitorowanie wydajności i stabilności klastra oraz wirtualnych maszyn.

10. **Zarządzanie i utrzymanie**:
    - Regularna aktualizacja oprogramowania serwerowego, systemu operacyjnego i wirtualizacyjnego. Zapewnienie kopii zapasowych danych wirtualnych maszyn i ich regularne odnawianie.

1. Segmentacja sieci:

Analiza infrastruktury sieciowej:
   - Dokładne zrozumienie architektury sieciowej, w tym topologii, urządzeń sieciowych i przepustowości.
2. **Identyfikacja zasobów i ich krytyczności:**
   - Określenie kluczowych zasobów sieciowych, takich jak serwery, bazy danych, urządzenia końcowe, które wymagają zabezpieczenia.
3. **Kategoryzacja użytkowników i urządzeń:**
   - Grupowanie użytkowników i urządzeń na podstawie ich roli, poziomu dostępu oraz wymagań dotyczących bezpieczeństwa.
4. **Projektowanie modelu segmentacji:**
   - Określenie, jakie zasoby i użytkownicy będą znajdować się w poszczególnych segmentach sieciowych.
   - Ustalenie polityk komunikacji między segmentami oraz zasady kontroli dostępu.
5. **Wybór odpowiednich technologii i narzędzi:**
   - Przegląd dostępnych rozwiązań do segmentacji sieci, takich jak firewalle, VLAN-y, routery, czy mikrosegmentacja.
   - Wybór narzędzi i technologii odpowiednich dla potrzeb firmy.
6. **Konfiguracja urządzeń sieciowych:**
   - Konfiguracja firewalle, routery, przełączniki VLAN i inne urządzenia sieciowe zgodnie z ustalonym modelem segmentacji.
   - Ustalenie reguł filtracji ruchu sieciowego między segmentami.
7. **Wdrożenie zabezpieczeń na poziomie aplikacji:**
   - Zaimplementowanie zabezpieczeń na poziomie aplikacji, takich jak zaporę ogniową, antywirusy, oprogramowanie wykrywające złośliwe oprogramowanie.
8. **Testowanie i weryfikacja:**
   - Przeprowadzenie testów, aby upewnić się, że segmentacja działa zgodnie z oczekiwaniami i nie wprowadza nieoczekiwanych problemów w dostępie do zasobów.
9. **Monitorowanie i zarządzanie:**
   - Ustawienie systemu monitorowania, który będzie śledził ruch w sieci oraz ewentualne naruszenia polityk segmentacji.
   - Regularne aktualizacje i zarządzanie politykami segmentacji w miarę zmian w infrastrukturze sieciowej.
10. **Szkolenie personelu:**

- Szkolenie personelu odpowiedzialnego za zarządzanie siecią w zakresie korzystania z nowej segmentacji oraz zasad bezpieczeństwa.

3. Wdrożenie oprogramowania do wykonywania kopii zapasowych.

1: Planowanie i Przygotowanie
- Określenie wymagań dotyczących backupu i replikacji, w tym ilość danych do przechowywania, czas przywracania, dostępność i inne czynniki.
- Weryfikacja posiadania odpowiedniej ilości przestrzeni dyskowej i zasobów sieciowych do przechowywania kopii zapasowych.
- Pobranie niezbędnego oprogramowania do wykonywania kopii zapasowych i przeczytanie jego dokumentacji.

2: Instalacja i Konfiguracja
- Uruchomienie instalatora wybranego oprogramowania do wykonywania kopii zapasowych na wybranym serwerze.
- Postępuj zgodnie z kreatorami instalacji, akceptując licencję, wybierając komponenty do zainstalowania i konfigurując ustawienia.
- Konfiguracja połączenia ze swoim środowiskiem wirtualizacji

3: Konfiguracja Backupu
- Konfiguracja planów backupu, określając harmonogramy, miejsca przechowywania i inne parametry.
- Wybranie, które maszyny wirtualne lub inne zasoby będą chronione za pomocą kopii zapasowych.
- Ustawienie retencji danych i polityki przechowywania, aby dostosować je do wymagań firmy.

4: Konfiguracja Replikacji (opcjonalnie)
- Konfiguracje odpowiedniego zadania replikacji, określając maszyny wirtualne źródłowe i docelowe, harmonogramy i inne parametry.
- Weryfikacja dostępności docelowego środowiska na przyjęcie replikowanych maszyn wirtualnych.

5: Testowanie i Wdrażanie
- Przetestowanie planów backupu i replikacji, aby upewnić się, że są one zgodne z oczekiwaniami i spełniają wymagania czasu przywracania.
- Wdrożenie skonfigurowanych i przetestowanych planów na produkcji, monitorując ich wydajność i skuteczność.

6: Monitorowanie i Administracja
- Regularne monitorowanie wykonywanych kopii zapasowych i replikacji, w celu weryfikacji ich poprawności i zgodności z planem.
- Weryfikacja raportów i dzienników zdarzeń oprogramowania do wykonywania kopii zapasowych, aby szybko reagować na jakiekolwiek problemy.

4. Wdrożenie systemów teleinformatycznych

Dostawa oraz wdrożenie oprogramowania typu SIEM

1. **Dostawa oraz wdrożenie oprogramowania typu SIEM + EDR**

2. Zamawiający na potrzeby instalacji i wdrożenia udostępni infrastrukturę na serwerach zwirtualizowanych, wg. specyfikacji uzgodnionych z Wykonawcą. Czynności związane z wdrożeniem systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja systemu przez Wykonawcę odbywać się będzie z wykorzystaniem środków komunikacji elektronicznej.

3.

4. Wykonawca zobowiązuje się do dostarczenia kompleksowego oprogramowania typu Security Information and Event Management (SIEM) oraz EDR (Endpoint Detection and Response), które będzie spełniało poniższe wymagania funkcjonalne i techniczne.

5.

2. Funkcjonalności systemu.
    1. Monitorowanie zdarzeń (logów) w trybie ciągłym.

2. Zbieranie zdarzeń z serwerów wirtualnych, fizycznych, Active Directory, przełączników oraz innych urządzeń w infrastrukturze Zamawiającego.
3. Agregacja i korelacja logów.
4. Wykrywanie ataków typu brute force i innych złośliwych działań.
5. Analiza logów w oparciu o wbudowane reguły bezpieczeństwa.
6. Możliwość tworzenia własnych reguł korelacji.
7. Konfigurowanie alertów o wysokim priorytecie w przypadku wykrycia podejrzanych zdarzeń.
8. Panel do wyszukiwania i analizy zdarzeń.
9. Możliwość integracji z innymi systemami bezpieczeństwa.
10. Przechowywanie logów z kluczowych zasobów przez okres 24 miesięcy.
11. Monitorowanie i ochrona punktów końcowych (np. komputerów, laptopów, serwerów).
12. Wykrywanie i blokowanie złośliwego oprogramowania.
13. Zapobieganie atakom typu ransomware.
14. Automatyczne reagowanie na incydenty bezpieczeństwa.
15. Dostęp do szczegółowych informacji o zdarzeniach na punktach końcowych.
16.

3. Wdrożenie systemu.
    1. Wykonawca będzie odpowiedzialny za instalację i konfigurację oraz optymalizację środowiska systemu w infrastrukturze Zamawiającego oraz opiekę serwisową i wsparcie techniczne przez okres 30 dni.
4. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:
    1. Przedstawienie architektury systemu.
    2. Omówienie procedur obsługi administracyjnej systemu;
    3. Omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń systemu;
    4. Przekazanie informacji na temat konfiguracji i zarządzania systemem;
    5. Instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną.

5. Wdrożenie systemów teleinformatycznych

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

A. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.
B. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.
C. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.
D. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.
E. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.
F. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania

działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.

G. Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.

H. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.

I. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.

J. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

- Numery kart kredytowych
- Numery IBAN
- Numery dowodów osobistych
- Polski numer paszportu
- Numer PESEL

K. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.

L. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.

M. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.

N. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.

O. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.

P. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.

Q. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

6. Utrzymanie systemów teleinformatycznych – 1 sztuka

Usługi stałego wsparcia technicznego (II linia wsparcia IT)
Przedmiotem zamówienia jest świadczenie usług stałej opieki informatycznej dla Zamawiającego, obejmujących w ilości 70 godzin oraz w okresie 12 miesięcy:

- pomoc zdalna w rozwiązywaniu problemów z serwerami i oprogramowaniem serwerowym;
- monitorowanie dostępności serwerów i usług;
- reagowanie na problemy związane z dostępnością serwerów;
- zarządzanie zmianami i wersjami oprogramowania serwerowego;
- instalacja i konfiguracja nowego oprogramowania i sprzętu;
- zarządzanie patchami i aktualizacjami oprogramowania;
- backup i odzyskiwanie danych;
- monitorowanie wydajności systemów i aplikacji;
- diagnozowanie i rozwiązywanie problemów z wydajnością;
- zarządzanie konfiguracją systemów i aplikacji;
- automatyzacja rutynowych zadań operacyjnych;
- analiza i interpretacja logów systemowych i aplikacji;
- reagowanie na alerty bezpieczeństwa generowane przez SIEM;
- analiza trendów i przewidywanie przyszłych problemów;
- wdrażanie i zarządzanie kontenerami i usługami mikrousług;
- konfiguracja i zarządzanie sieciami wirtualnymi;
- zarządzanie certyfikatami SSL/TLS;

- wdrażanie zasad bezpieczeństwa i konfiguracji firewalli;
- audyt konfiguracji i zabezpieczeń systemów;
- przeprowadzanie testów penetracyjnych i ocen ryzyka;
- zarządzanie użytkownikami i uprawnieniami;
- zarządzanie bazami danych (backup, tuning, aktualizacje);
- zarządzanie środowiskami deweloperskimi, testowymi i produkcyjnymi;
- wsparcie dla procesów CI/CD (Continuous Integration/Continuous Deployment);
- doradztwo w zakresie architektury systemów i aplikacji;
- optymalizacja kosztów usług chmurowych;
- zarządzanie kluczami szyfrowania i dostępem do danych wrażliwych;
- planowanie i testowanie ciągłości działania (DR/BCP);
- zarządzanie incydentami bezpieczeństwa i reagowanie na nie;
- konsultacje w zakresie najlepszych praktyk DevOps i bezpieczeństwa IT;
- analiza przyczynowa (Root Cause Analysis) dla incydentów IT;
- zarządzanie dokumentacją techniczną i operacyjną;
- wsparcie przy migracjach systemów i aplikacji;
- ocena zgodności z wymaganiami regulacyjnymi i standardami branżowymi;
- szkolenia użytkowników i personelu technicznego w zakresie obsługi systemów;
- monitorowanie zagrożeń w cyberprzestrzeni i aktualizacja zabezpieczeń;
- zarządzanie konfiguracją sieci i urządzeń sieciowych;
- ocena skuteczności zaimplementowanych środków bezpieczeństwa;
- wsparcie dla procesów skalowania infrastruktury IT;
- analiza potrzeb biznesowych i doradztwo technologiczne;
- optymalizacja procesów biznesowych za pomocą technologii IT;
- przeglądy architektury systemów pod kątem najlepszych praktyk i zaleceń;
- wsparcie w zakresie integracji systemów i aplikacji;
- zarządzanie środowiskami wirtualnymi i chmurowymi;
- ocena wykorzystania zasobów IT i rekomendacje dotyczące optymalizacji;
- zarządzanie zmianą w infrastrukturze IT i procesach operacyjnych.

Zadania będą realizowane selektywnie i niezwłocznie na każde wezwanie Zamawiającego w godzinach 8:00 – 16:00 oraz w przypadku problemów krytycznych, przez całą dobę.

7. Testy penetracyjne

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.
Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:

- wykonanie skanowań z wykorzystaniem wbudowanych szablonów;
- skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi);
- weryfikacje domyślnych haseł według zadanego słownika;
- skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy i aplikacje) oraz weryfikację uprawnień zadanego użytkownika;
- ustawienia harmonogramu skanowań;
- możliwość porównania wyników poszczególnych skanowań;
- możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (w tym HTML, CVS i XML);
- możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności i możliwość sortowania po IP i podatnościach.

Aplikacje do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:

- przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
- przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;

- dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
- wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
- tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
- precyzyjna konfiguracja reguł przechwytywania wiadomości;
- możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;
- pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
- żądania i odpowiedzi dostępne w edytorze http;
- narzędzie do ręcznej edycji i ponownego wstawiania żądań;
- narzędzie do analizy statystycznej tokenów sesji;
- możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz powrót do zapisanego miejsca;
- biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;
- możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;
- skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
- możliwość analizy docelowej aplikacji internetowych.
- narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.

Potencjał osobowy przedstawia się poprzez posiadanie przez osoby testujące łącznie takie certyfikaty jak: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity), eCPPT (eLearnSecurity). Skanowania nie mogą być realizowane tylko z wykorzystaniem narzędzi automatycznych, konieczna jest manualna weryfikacja podatności znalezionych w testach automatycznych. Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.

W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

1. Rekonesans.
   1. Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję w celu stworzenia potencjalnej bazy loginów i haseł.
   2. Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi).
   3. zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych.
   4. Sprawdzenie występowania w wyciekach znalezionych loginów.
2. Enumeracja zasobów.
   1. Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz z określeniem ich wersji) działających w ramach usług.
   2. Skanowanie publicznej infrastruktury.
   3. Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.
   4. Sprawdzenie udostępnionych w sieci wewnętrzej plików i folderów w szczególności pod kątem występowania danych wrażliwych.
   5. Analiza dostępnych wewnątrz sieci, usług, protokołów i urządzeń.
3. Eksploitacja.
   1. Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.
   2. Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) – po uzgodnieniu z Zamawiającym.
   3. Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).
4. Eskalacja uprawnień.

1. Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.
2. Rozpoznanie zasobów wewnętrznych, przechodzenie na inne środowiska dostępne ze skompromitowanych w pkt.3 zasobów (lateral movement).

5. Raport z testu penetracyjnego.

Wykonawca dostarczy raport zawierający:

1. Podsumowanie dla kierownictwa.
2. Opis zakresu wykonanych prac.
3. Wyłączenia z testów jeżeli były.
4. Listę danych zebranych w trakcie rekonesansu (w tym listę zidentyfikowanych adresów IP w sieci wewnętrznej).
5. Listę znalezionych podatności wraz z określoną dla niej waga zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.
6. Szczegółowy opis znalezionych podatności.
7. Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.

8. Szkolenia powiązane z testami socjotechnicznymi

1. Przygotowanie kampanii socjotechnicznej;
   a. wybór i zakup przez Wykonawcę domeny (łudząco podobnej do domeny Zamawiającego), która zostanie wykorzystana do kampanii socjotechnicznej;
   b. opracowanie bazy mailingowej pracowników objętych kampanią socjotechniczną oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłośliwy kod pozwalający na mierzenie efektów kampanii;
   c. wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);
   d. wsparcie w zakresie dodania domeny wybranej do przeprowadzenia kampanii socjotechnicznej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców).
2. Przygotowanie spreparowanych zasobów służących wyłudzaniu informacji:
   a. serwer strony www z bazą danych powiązany z domeną, która została zakupiona w celu przeprowadzenia kampanii socjotechnicznej;
   b. wykonanie kopii strony internetowej Zamawiającego i umieszczenie jej pod spreparowanym adresem;
   c. wygenerowanie niezbędnych certyfikatów SSL;
   d. przygotowanie spreparowanego aktywnego dokumentu PDF, wyposażonego w autorski, niezłośliwy skrypt, którego celem jest zebranie informacji o użytkownikach, którzy dokonali otwarcia pliku PDF i uruchomienia niezłośliwego skryptu (w prawdziwej kampanii byłoby to złośliwe oprogramowanie);
   e. utworzenie nowej podstrony, na której umieszczony zostanie spreparowany plik PDF;
   f. przygotowanie konta mailowego, którego celem jest podszycie się pod jedną z osób wtajemniczonych w prowadzone testy phishingowe;
   g. przygotowanie treści wiadomości e-mail i wyposażenie jej w mechanizmy pozwalające na przeprowadzenie tzw. detekcji umiejscowienia (uzyskanie adresu IP potencjalnej „ofiary").
3. Przeprowadzenie kampanii socjotechnicznej (wysłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej).
4. Wykonanie raportu z testu socjotechnicznego w języku polskim.
5. Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa, ukierunkowanego na omówienie wyników kampanii socjotechnicznej oraz co najmniej:
   a. wprowadzenie do cyberbezpieczeństwa:
      - czym jest cyberbezpieczeństwo;
      - dlaczego cyberbezpieczeństwo jest ważne;
      - kluczowe zagadnienia związane z cyberbezpieczeństwem;

11.	Zasady Listy Kontroli Dostępu (ACL)	512
12.	IGMP snooping	Tak
13.	Ochrona hasłem	Tak
14.	obsługuje SSH/SSL	Tak
15.	Filtrowanie adresów MAC	Tak
16.	Szyfrowanie / bezpieczeństwo	HTTPS, SSH, SSL/TLS
III.	**PORTY I INTERFEJSY**	
17.	Podstawowe przełączanie RJ-45 Liczba portów Ethernet	48
18.	Podstawowe przełączania Ethernet RJ-45 porty typ	Gigabit Ethernet (10/100/1000)
19.	Ilość slotów Modułu SFP+	4
20.	Liczba portów USB 2.0	1
IV.	**SIEĆ**	
21.	Standardy komunikacyjne	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1ad, IEEE 802.1af, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3u

22.	Dublowanie portów	Tak
23.	Protokół drzewa rozpinającego	Tak
24.	Blokowanie head-of-line (HOL)	Tak
25.	Prędkość transferu danych przez Ethernet LAN	1000 Mbit/s
26.	Kontrola wzrostu natężenia ruchu	Tak
27.	Automatyczne MDI/MDI-X	Tak
28.	Podpora kontroli przepływu	Tak
29.	Obsługa sieci VLAN	Tak
30.	Liczba VLANs	255
V.	**PRZESYŁANIE DANYCH**	
31.	Wielkość tabeli adresów	8000 wejścia
32.	Zgodny z Jumbo Frames	Tak
33.	Rozszerzenie Jumbo Frames	9000

VI.	**FUNKCJE MULTICAST**	
34.	Obsługa Multicast	Tak
VII.	**PROTOKOŁY**	
35.	Protokoły zarządzające	SNMP
VIII.	**KONSTRUKCJA**	
36.	Możliwości montowania w stelażu	Tak
37.	Przycisk reset	Tak
38.	Diody LED	Tak
IX.	**WYDAJNOŚĆ**	
39.	Procesor wbudowany	Tak
40.	Taktowanie procesora	800 MHz
41.	Pojemność pamięci wewnętrznej	512 MB
42.	Wielkość pamięci flash	256 MB

43.	Aktualizacje oprogramowania urządzenia	Tak
X.	**MOC**	
44.	Zasilacz dołączony	Tak
45.	Częstotliwość wejściowa AC	50 - 60 Hz
XI.	**WARUNKI PRACY**	
46.	Zakres temperatur (eksploatacja)	-5 - 50 °C
47.	Zakres temperatur (przechowywanie)	-25 - 70 °C
48.	Zakres wilgotności względnej	10 - 90%
49.	Dopuszczalna wilgotność względna	10 - 90%

6. Zarządzane urządzenia sieciowe z obsługą VLAN – 2 sztuki.

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

- Ilość portów 8 portów SFP+ oraz 8 portów 10GBaseT niezależne
- Chłodzenie od przedu do tyłu obudowy
- Tablica MAC min. 16K

- Tablica ARP/NDP min. 888
- Bufor 16Mb
- MTBF min. 196120 godzin
- Wydajność min. 238 Mp/s
- Przepustowość min. 320 Gb/s
- Port USB
- Port miniUSB
- Port zarządzania Out-of-band;
- Web GUI
- HTTPs
- CLI
- Telnet
- SSH
- SNMP
- MIB RSPAN
- Radius
- TACACS+
- DiffServ
- Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
- IPv4/IPv6 Multicast filtering
- IGMPv3 MLDv2 Snooping
- ASM & SSM
- IGMPv1,v2 Querier
- Auto-VoIP
- Auto-iSCSI
- Policy-based routing (PBR)
- LLDP-MED
- Spanning Tree
- Green Ethernet
- STP
- MTP
- RSTP
- PV(R)STP
- BPDU/STRG Root Guard
- EEE (802.3az)
- GVRP/GMRP
- Q in Q,
- Private VLAN

- DOT1X
- MAB
- Captive Portal
- DHCP Snooping
- Dynamic ARP
- Inspection
- IP Source Guard
- CPU min 800 Mhz
- Min 1GB RAM
- Min 256MB Flash
- Min ilość obsługiwanych VLAN 4K
- DHCP Server min 2K rezerwacji
- sFlow
- Minimalna ilość przełączników w stosie: 8
- Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
- Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
- Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
- Non-stop forwarding (NSF)
- Distributed Link Aggregation (LAGs across the stack)
- Ilość interfejsów IP 128
- Double VLAN Tagging (QoQ)
- Yes
- PIM-DM (Multicast Routing - dense mode)
- PIM-DM (IPv6)
- PIM-SM (Multicast Routing - sparse mode)
- PIM-SM (IPv6)
- RIPv1
- RIPv2
- OSPFv2
- RFC 2328
- RFC 1583
- OSPFv3
- OSPFv2 min. sąsiadów 400
- OSPFv3 min. sąsiadów 400
- OSPFv3 min. sąsiadów na interfejs 100
- UDLD
- LLPF

- DHCPv6 Snooping
- wysyłanie alertów na email
- MMRP
- Ilość ACL min. 100
- Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu

7. Oprogramowanie serwera – 2 sztuki.

Licencje systemu operacyjnego Microsoft Windows Server 2022 Datacenter 16-core lub oprogramowania równoważnego nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji. Licencje nie mogą być dedykowane tylko do jednego producenta sprzętu serwerowego.

RÓWNOWAŻNOŚĆ:

1. Warunki równoważności dla licencji systemu Microsoft Windows Server 2022 Datacenter.

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Datacenter, Zamawiający wymaga dostarczenia licencji dla 2 serwerów oraz instalacji i migracji obecnego środowiska. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:

1) Współpraca z procesorami o architekturze x86 – 64bit.
2) Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3) Możliwość budowania klastrów składających się z 64 węzłów.
4) Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 16 rdzeni.
5) Praca w roli klienta domeny Microsoft Active Directory.
6) Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7) Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8) Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9) Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10) Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11) Możliwość uruchomienia roli serwera stron WWW.
12) W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13) W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14) Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną

licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

15) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
18) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
19) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
20) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
21) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
22) Możliwość wykorzystania standardu http/2.
23) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
24) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
25) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
26) Mechanizmy logowania w oparciu o: a) login i hasło,
    a) karty z certyfikatami (smartcard),
    b) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
27) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
    a) określonych grup użytkowników,
    b) zastosowanej klasyfikacji danych,
    c) centralnych polityk dostępu w sieci,
    d) centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
28) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
29) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
30) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie

zdefiniowanego zestawu polityk bezpieczeństwa.

31) Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
32) Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
33) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
        - bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,
    c) zdalna dystrybucja oprogramowania na stacje robocze,
    d) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
    e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        - Dystrybucję certyfikatów poprzez http,
        - Konsolidację CA dla wielu lasów domeny,
        - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f) szyfrowanie plików i folderów,
    g) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
    h) szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
    i) możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
    j) serwis udostępniania stron WWW,
    k) wsparcie dla protokołu IP w wersji 6 (IPv6),
    l) wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m) wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),

n) możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

o) możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.

p) mechanizmy wirtualizacji mające 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,
- możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

q) możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.

r) wsparcie dla rozwiązania Kubernetes.

s) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz

z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

t) wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

u) mechanizmy deduplikacji i kompresji na wolumenach.

v) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

w) mechanizm konfiguracji połączenia VPN do platformy Azure.

x) wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.

y) mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.

z) możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

8. Oprogramowanie do wykonywania kopii zapasowych – 20 licencji uniwersalnych.

Licencja musi być na bezterminowa, bez żadnych dodatkowych opłat a wsparcie na minimum 12 miesięcy.

Lp.	Minimalne wymagania Zamawiającego

	I. Wymagania ogólne
1.	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
2.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
3.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
	II. Całkowite koszty posiadania
1.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
2.	Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3.	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.
4.	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.
5.	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.

6.	Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
7.	Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
8.	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9.	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)
10.	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
11.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
12.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
13.	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
14.	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
15.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

16.	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
	III. **Wymagania RPO**
1.	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
2.	Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3.	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
4.	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.
5.	Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
6.	Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
7.	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
8.	Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

9.	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
10.	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
11.	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.
12.	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.
13.	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
14.	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
15.	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
IV.	**Wymagania RTO**
1.	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.

2.	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)
3.	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
4.	Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
5.	Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
6.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
7.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
8.	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
9.	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.
10.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell

11.	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
12.	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
13.	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.
14.	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.
15.	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.
16.	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.
17.	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.
18.	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.
19.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

20.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
21.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
22.	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
V.	**Ograniczenie ryzyka**
1.	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)
2.	Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
3.	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
4.	Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
5.	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
VI.	**Środowiska fizyczne**

1.	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
2.	Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
3.	Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
4.	Rozwiązanie musi wspierać system operacyjny macOS
5.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
6.	Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
7.	Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
8.	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
9.	Rozwiązanie musi wspierać backup podłączonych dysków USB

10.	Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
11.	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)
12.	Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
13.	Rozwiązanie musi wspierać kontrolę pasma sieciowego
14.	Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
15.	Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
16.	Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
17.	Rozwiązanie musi wspierać technologię BitLocker
18.	Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania

19.	Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
20.	Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
21.	Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
22.	Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
23.	Rozwiązanie musi wspierać szyfrowanie
24.	Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
25.	Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
26.	Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
27.	Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

- przegląd statystyk i trendów w cyberbezpieczeństwie.

b. typy zagrożeń w cyberprzestrzeni:
   - malware (wirusy, trojany, robaki itp.);
   - ataki typu phishing i spear phishing;
   - ataki DDoS;
   - ataki ransomware;
   - zagrożenia związane z sieciami społecznościowymi.

c. zasady bezpieczeństwa i praktyki:
   - zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
   - zasady bezpieczeństwa e-mail;
   - bezpieczeństwo w sieciach bezprzewodowych;
   - bezpieczne przeglądanie internetu;
   - backup i odzyskiwanie danych.

d. reagowanie na incydenty i planowanie awaryjne:
   - jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
   - zasady reagowania na incydenty;
   - planowanie awaryjne i kontynuacja działalności;
   - Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

Czas trwania szkolenia przewidziano na co najmniej dwie grupy po 4 godziny robocze z uwzględnieniem przerw 15 minut w każdym szkoleniu. Po szkoleniu Wykonawca udostępni co najmniej 30 minut na pytania i odpowiedzi uczestników.

9. Warsztaty SZBI.

W ramach warsztatów z osobą prowadzącą dotyczącym Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), przewiduje się przegląd oraz omówienie przykładowej dokumentacji SZBI. Uczestnicy warsztatów będą również zaangażowani w proces tworzenia nowej dokumentacji, dostosowanej do specyficznych potrzeb organizacji, zgodnie z obowiązującymi normami i wymogami. Warsztaty mają na celu przekazanie wiedzy z zakresu opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. .

Dokumentacja musi zawierać następujące kryteria:

1. **Ewidencja Obszaru Przetwarzania Informacji:**

- Dokument musi zawierać ewidencję obszarów przetwarzania informacji, obejmującą lokalizacje wraz z oznaczeniami, nazwami, kondygnacjami i adresami.
- Dokument powinien służyć do monitorowania i zarządzania miejscami, w których przetwarzane są chronione informacje.

2. **Wprowadzenie do Systemu Zarządzania Bezpieczeństwem informacji**

- Dokument musi definiować podstawowe zasady Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym ochronę aktywów informacyjnych, monitorowanie ryzyk oraz wdrażanie zabezpieczeń.

- Dokument powinien opisywać procesy zarządzania bezpieczeństwem informacji, bazujące na cyklu PDCA (Plan-Do-Check-Act), obejmujące szacowanie ryzyka, monitorowanie skuteczności zabezpieczeń i ich doskonalenie.

3. Terminy stosowane w Systemie Zarządzania Bezpieczeństwem Informacji

- Dokument musi zawierać definicje terminów stosowanych w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI), takich jak ryzyko, aktywa informacyjne, incydent bezpieczeństwa oraz cyberbezpieczeństwo.
- Każdy termin powinien być dokładnie opisany, uwzględniając jego znaczenie oraz zastosowanie w kontekście zarządzania bezpieczeństwem informacji.

4. Kontekst Organizacji

- Dokument musi opisywać czynniki zewnętrzne i wewnętrzne wpływające na organizację w kontekście Systemu Zarządzania Bezpieczeństwem Informacji, w tym aspekty prawne, regulacyjne, technologiczne, społeczne oraz finansowe.
- Dokument powinien określać zakres Systemu Zarządzania Bezpieczeństwem Informacji, uwzględniając lokalizacje, procesy, zasoby oraz jednostki organizacyjne, które są objęte systemem.

5. Zarządzanie Ryzykiem w Bezpieczeństwie informacji

- Dokument musi opisywać proces zarządzania ryzykiem w bezpieczeństwie informacji, obejmujący identyfikację, analizę, ocenę oraz postępowanie z ryzykiem, w tym kryteria oceny ryzyka i akceptacji ryzyka.
- Dokument powinien definiować metodykę szacowania ryzyka, w tym sposób określania prawdopodobieństwa, skutków oraz przypisywania wartości ryzyka, a także wytyczne dotyczące akceptowania, monitorowania i przeglądu ryzyka.

6. Instrukcja Szacowania i Postępowania z Ryzykiem w Bezpieczeństwie Informacji

- Instrukcja musi opisywać proces szacowania i postępowania z ryzykiem w bezpieczeństwie informacji, obejmujący identyfikację zagrożeń, podatności oraz aktywów i ich zabezpieczeń, których ryzyko dotyczy.
- Dokument powinien zawierać szczegółowe wytyczne dotyczące analizy ryzyka, w tym oszacowanie następstw, prawdopodobieństwa, poziomów ryzyka oraz metody określania i dokumentowania działań w zakresie postępowania z ryzykiem.

7. Działania odnoszące się do Ryzyk i Szans Systemu Zarządzania Bezpieczeństwem Informacji.

- Dokument musi opisywać działania odnoszące się do zidentyfikowanych ryzyk i szans w Systemie Zarządzania Bezpieczeństwem Informacji, w tym określenie sposobów realizacji działań oraz ich integrację z procesami SZBI.
- Dokument powinien zawierać wytyczne dotyczące oceny skuteczności działań, uwzględniając monitorowanie, pomiary, audyty oraz przeglądy zarządzania, aby zapewnić zgodność z wymaganiami prawnymi oraz bezpieczeństwo informacji.

8. Deklaracja Stosowania Opracowana

- Dokument musi zawierać wykaz zabezpieczeń stosowanych w Systemie Zarządzania Bezpieczeństwem Informacji, wraz z uzasadnieniem ich wyboru oraz oceną wdrożenia lub wyłączenia, zgodnie z Załącznikiem A normy ISO/IEC 27001.
- Dokument powinien opisywać sposób wdrożenia zabezpieczeń, wskazując ich cel, specyfikę działalności oraz wyniki analizy ryzyka, a także uzasadniać ewentualne wyłączenia zabezpieczeń.

9. Cele bezpieczeństwa informacji

- Dokument musi określać cele bezpieczeństwa informacji, które obejmują zarządzanie ryzykiem, incydentami, zgodność z przepisami oraz zapewnienie ciągłości działania i bezpieczeństwa aktywów.
- Dokument powinien zawierać mierzalne wskaźniki realizacji celów, w tym liczbę audytów, szkoleń, zgłoszeń incydentów, a także utrzymywanie odpowiednich rejestrów i ewidencji aktywów.

10. Plan osiągniecia Celów Bezpieczeństwa Informacji

- Dokument musi zawierać plan realizacji celów bezpieczeństwa informacji, określając zadania, wskaźniki oraz harmonogram ich realizacji i weryfikacji, zgodnie z raportami z monitorowania i pomiarów systemu zarządzania bezpieczeństwem informacji.
- Plan powinien przypisywać odpowiedzialność za realizację poszczególnych zadań oraz wskazywać kluczowe cele, takie jak zarządzanie ryzykiem, incydentami, ciągłością działania oraz zgodność z wymaganiami prawnymi i regulacyjnymi.

11. Monitorowanie, Pomiary, Analiza i Ocena Systemu Zarządzania Bezpieczeństwem Informacji

- Dokument musi opisywać proces monitorowania, pomiarów, analizy i oceny Systemu Zarządzania Bezpieczeństwem Informacji, obejmujący zgodność z wymaganiami prawnymi oraz skuteczność w osiąganiu celów bezpieczeństwa informacji.
- Dokument powinien zawierać wskaźniki monitorowania oraz określać odpowiedzialność Pełnomocnika ds. Bezpieczeństwa Informacji za utrzymywanie raportów i ich przekazywanie Najwyższemu Kierownictwu.

12. Raport z Monitorowania, Pomiarów, Analizy i Oceny Systemu Zarządzania Bezpieczeństwem informacji

- Raport musi zawierać wyniki monitorowania, pomiarów, analizy i oceny Systemu Zarządzania Bezpieczeństwem Informacji, w tym liczbę audytów, działań zaradczych, incydentów oraz wskaźniki ryzyka i zgodności z wymaganiami prawnymi.
- Dokument powinien zawierać przegląd zapisów i wskaźników monitorowania z poprzedniego roku oraz przypisywać odpowiedzialność za realizację poszczególnych działań związanych z zarządzaniem bezpieczeństwem informacji.

13. Raport z Audytu Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji

- Raport z audytu wewnętrznego musi zawierać ocenę zgodności Systemu Zarządzania Bezpieczeństwem Informacji z wymaganiami prawnymi i regulacyjnymi, a także oceniać jego skuteczność w osiąganiu zamierzonych celów.
- Dokument powinien przedstawiać ustalenia audytu, w tym wykryte zgodności i niezgodności, dowody potwierdzające oraz zalecenia audytora dotyczące doskonalenia systemu.

14. Audyty Wewnętrzne Systemu Zarządzania Bezpieczeństwem Informacji

- Dokument musi definiować zasady i procedury przeprowadzania audytów wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z normami ISO oraz wymogami prawnymi, w tym zasady rzetelności, poufności, niezależności i podejścia opartego na dowodach.
- Dokument powinien opisywać zarządzanie programem audytów, w tym jego tworzenie, zatwierdzanie, przygotowanie planów audytów, przeprowadzanie działań audytowych oraz działania poaudytowe, wraz z odpowiedzialnością za realizację i doskonalenie audytów.

15. Plan Audytu Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji.

- Plan Audytu Wewnętrznego musi określać cele, zakres, kryteria oraz metody przeprowadzania audytu, w tym audyty na miejscu i zdalne, a także analizę dokumentów, obserwację pracy i rozmowy z personelem.
- Dokument powinien zawierać informacje o odpowiednich wymaganiach prawnych i regulacyjnych, procesach do audytu, oraz wskazywać lokalizacje i osoby odpowiedzialne za poszczególne etapy audytu.

16. Program Audytów Wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji

- Program Audytów Wewnętrznych musi zawierać liczbę i rodzaje zaplanowanych audytów, ich cele, zakres oraz kryteria, zgodnie z wymaganiami prawnymi i regulacyjnymi dotyczącymi Systemu Zarządzania Bezpieczeństwem Informacji.
- Dokument powinien definiować metody audytu, takie jak wizyty, przegląd dokumentów, rozmowy oraz analizę danych, a także przypisywać odpowiedzialność za realizację audytów Pełnomocnikowi ds. Bezpieczeństwa Informacji.

17. Przegląd Zarządzania

- Dokument Przegląd Zarządzania musi zawierać coroczną ocenę przydatności, adekwatności i skuteczności Systemu Zarządzania Bezpieczeństwem Informacji, w tym analizę działań korygujących, doskonalących oraz wdrożonych w wyniku incydentów i audytów wewnętrznych.
- Dokument powinien obejmować przegląd zmian czynników zewnętrznych i wewnętrznych, analizę wyników monitorowania systemu, cele bezpieczeństwa oraz informacje zwrotne od stron zainteresowanych.

18. Raport z Przeglądu Zarządzania

- Raport z Przeglądu Zarządzania musi zawierać ocenę działań podjętych po wcześniejszych przeglądach zarządzania, analizę czynników zewnętrznych i wewnętrznych oraz informacje o działaniach korygujących i doskonalących w obszarze bezpieczeństwa informacji.
- Dokument powinien obejmować wyniki audytów wewnętrznych, analizę celów bezpieczeństwa informacji, a także możliwości doskonalenia systemu wynikające z raportów oraz przeglądów.

19. Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji

- Dokument musi opisywać procedury identyfikacji, korygowania i doskonalenia niezgodności w Systemie Zarządzania Bezpieczeństwem Informacji, w tym działania eliminujące przyczyny niezgodności oraz ocenę skuteczności wdrożonych środków korygujących.
- Dokument powinien obejmować proces ciągłego doskonalenia systemu poprzez regularne przeglądy, monitorowanie, analizę oraz raportowanie działań doskonalących i korygujących.

20. Polityka Bezpieczeństwa Informacji

- Polityka Bezpieczeństwa Informacji musi określać ogólne kierunki i wytyczne w zakresie ochrony informacji, w tym zarządzanie poufnością, integralnością, dostępnością oraz innymi atrybutami bezpieczeństwa, takimi jak autentyczność, rozliczalność i niezaprzeczalność.
- Dokument powinien obejmować zasady zarządzania ryzykiem, incydentami oraz ciągłością bezpieczeństwa informacji, a także uwzględniać wymagania prawne, regulacyjne i umowne, zgodnie z przyjętymi celami bezpieczeństwa informacji.

21. Raport z Przeglądu Udokumentowanych Informacji Systemu Zarządzania Bezpieczeństwem Informacji

- Raport z Przeglądu Udokumentowanych Informacji musi obejmować ocenę zgodności udokumentowanych informacji Systemu Zarządzania Bezpieczeństwem Informacji, zidentyfikowane modyfikacje oraz propozycje aktualizacji w przypadku stwierdzenia potrzeby zmiany.
- Dokument powinien zawierać przegląd poszczególnych polityk, procedur, rejestrów i planów, w tym propozycje aktualizacji wynikające z analizy ryzyk, audytów wewnętrznych i przeglądów zarządzania.

22. Rejestr Właścicieli Udokumentowanych Informacji Systemu Zarządzania Bezpieczeństwem Informacji

- Rejestr Właścicieli Udokumentowanych Informacji musi zawierać wykaz dokumentów Systemu Zarządzania Bezpieczeństwem Informacji wraz z przypisanymi do nich właścicielami, odpowiedzialnymi za ich utrzymanie, aktualizację i zgodność z systemem.
- Dokument powinien wskazywać funkcje i stanowiska osób odpowiedzialnych za poszczególne udokumentowane informacje, aby zapewnić nadzór i odpowiedzialność nad ich prawidłowym zarządzaniem.

23. Role, Odpowiedzialność i Uprawnienia w Systemie Zarządzania Bezpieczeństwem Informacji

- Dokument musi definiować role, odpowiedzialność i uprawnienia związane z zarządzaniem bezpieczeństwem informacji, w tym Najwyższe Kierownictwo, Pełnomocnika ds. Bezpieczeństwa Informacji, Inspektora Ochrony Danych, Administratora Systemów Informatycznych oraz inne osoby przetwarzające informacje.
- Dokument powinien określać obowiązki związane z nadzorem nad zarządzaniem ryzykiem, incydentami, bezpieczeństwem aktywów, a także zobowiązania do raportowania, przeglądów i doskonalenia systemu zarządzania bezpieczeństwem informacji.

24. Polityka Stosowana Urządzeń Mobilnych

- Polityka Stosowania Urządzeń Mobilnych musi określać zasady zarządzania i zabezpieczania urządzeń mobilnych oraz zewnętrznych nośników danych, w tym autoryzację ich użytkowania poza organizacją, zgodnie z wymaganiami Polityki Zarządzania Aktywami.
- Dokument powinien zawierać wytyczne dotyczące ochrony informacji przechowywanych w urządzeniach mobilnych, w tym ich szyfrowania, zabezpieczania przed utratą, kradzieżą lub nieuprawnionym dostępem, zgodnie z Polityką Kryptografii i innymi regulacjami bezpieczeństwa.

25. Polityka Pracy Zdalnej

- Polityka Pracy Zdalnej musi określać zasady świadczenia pracy zdalnej, w tym wytyczne dotyczące zabezpieczenia aktywów oraz informacji przetwarzanych poza siedzibą organizacji, zgodnie z wymaganiami prawnymi i regulacyjnymi.

- Dokument powinien zawierać wytyczne dotyczące kontroli bezpieczeństwa, użycia narzędzi pracy oraz odpowiednich zabezpieczeń technicznych i organizacyjnych, zapewniając ochronę danych osobowych oraz tajemnic prawnie chronionych.

26. Polityka Bezpieczeństwa Zasobów Ludzkich

- Polityka Bezpieczeństwa Zasobów Ludzkich musi określać zasady zarządzania personelem w zakresie bezpieczeństwa informacji, w tym procesy rekrutacji, szkolenia, świadomości oraz procedury postępowania przed, w trakcie i po zakończeniu zatrudnienia.
- Dokument powinien zawierać wytyczne dotyczące weryfikacji kandydatów, nadawania i odbierania uprawnień, zarządzania incydentami bezpieczeństwa oraz zobowiązań personelu do przestrzegania zasad bezpieczeństwa informacji, także po zakończeniu zatrudnienia.

27. Wniosek o Nadanie, Zmianę lub Odebranie Dostępu do Systemów Informatycznych

- Wniosek o Nadanie, Zmianę lub Odebranie Dostępu do Systemów Informatycznych musi zawierać dane dotyczące systemów informatycznych, w tym nazwę systemu, identyfikator użytkownika oraz dane uwierzytelniające, a także określać rodzaj wnioskowanej operacji (nadanie, zmiana, odebranie dostępu).
- Dokument powinien być zatwierdzany przez kierującego jednostką organizacyjną oraz Administratora Systemów Informatycznych, potwierdzając nadanie, zmianę lub odebranie dostępu do wskazanych systemów.

28. Oświadczenie o Przestrzeganiu Wymagań Dotyczących Bezpieczeństwa Informacji

- Oświadczenie o Przestrzeganiu Wymagań Dotyczących Bezpieczeństwa Informacji musi zobowiązywać pracowników do przestrzegania wymagań prawnych, regulacyjnych i umownych dotyczących bezpieczeństwa informacji, w tym ochrony danych osobowych.
- Dokument powinien określać obowiązek stosowania środków technicznych i organizacyjnych, zgłaszania incydentów oraz zachowania poufności przetwarzanych informacji, także po zakończeniu współpracy.

29. Upoważnienie do Przetwarzania Informacji

- Upoważnienie do Przetwarzania Informacji musi zawierać dane osoby upoważnionej, stanowisko, funkcję oraz zakres przetwarzania informacji, w tym procesy i cele przetwarzania, a także daty obowiązywania upoważnienia.
- Dokument powinien być podpisany przez osobę upoważniającą oraz osobę upoważnioną, potwierdzając wydanie i odbiór upoważnienia, a wszelkie wcześniejsze upoważnienia tracą ważność.

30. Polityka Zarządzania Aktywami

- Polityka Zarządzania Aktywami musi definiować zasady inwentaryzacji, klasyfikacji oraz odpowiedzialności za aktywa organizacji, w tym identyfikację właścicieli aktywów i procedury zarządzania nimi w celu zapewnienia ich ochrony.
- Dokument powinien zawierać wytyczne dotyczące bezpiecznego użytkowania, przechowywania oraz wycofywania aktywów, w tym nośników informacji, zgodnie z wymaganiami prawnymi i regulacyjnymi.

31. Ewidencja Aktywów Podstawowych

- Ewidencja Aktywów Podstawowych musi zawierać identyfikację procesów, ich właścicieli oraz szczegółowe dane na temat rodzaju i typów procesów, w tym cele przetwarzania informacji, źródła danych, metody monitorowania oraz kontrolowania przebiegu procesów.
- Dokument powinien zawierać opisy mierników wejściowych i wyjściowych oraz określać powiązania między procesami, wskazując na ich wpływ i zależności, a także odpowiedzialność za nadzór nad aktywami i ich bezpieczeństwo.

32. Ewidencja Obszaru Przetwarzania Informacji

- Ewidencja Obszaru Przetwarzania Informacji musi zawierać oznaczenia, lokalizacje, kondygnacje oraz adresy fizycznych miejsc, w których przetwarzane są informacje w ramach Systemu Zarządzania Bezpieczeństwem Informacji.
- Dokument powinien umożliwiać identyfikację obszarów przetwarzania informacji, co pozwala na ich ewidencjonowanie i nadzór nad bezpieczeństwem fizycznym przetwarzanych danych.

33. Polityka Kontroli Dostępu

- Polityka Kontroli Dostępu musi definiować zasady autoryzacji i ograniczania dostępu do aktywów oraz informacji, zgodnie z wymaganiami prawnymi, regulacyjnymi i umownymi, aby zapewnić, że dostęp mają tylko uprawnieni użytkownicy.
- Dokument powinien obejmować procedury bezpiecznego logowania, zarządzania hasłami, kontrolę dostępu do systemów i aplikacji oraz odpowiedzialność użytkowników za poufne informacje uwierzytelniające.

34. Wymagania w Dostępie do Aktywów dla Personelu

- Dokument Wymagania w Dostępie do Aktywów dla Personelu musi określać zasady przyznawania dostępu do aktywów wyłącznie dla uprawnionych osób, zgodnie z nadanymi upoważnieniami oraz zabezpieczeniami wdrożonymi w organizacji.
- Dokument powinien zawierać wytyczne dotyczące zabezpieczania nośników informacji, stosowania polityki czystego biurka i ekranu, a także obowiązek zgłaszania incydentów bezpieczeństwa zgodnie z Polityką Zarządzania Incydentami.

35. Wymagania w Dostępie do Aktywów dla Podmiotów Zewnętrznych

- Dokument Wymagania w Dostępie do Aktywów dla Podmiotów Zewnętrznych musi określać zasady dostępu podmiotów zewnętrznych do aktywów organizacji, ograniczając dostęp do zakresu niezbędnego do realizacji określonych działań zgodnie z umowami, w tym Umowami o Zachowaniu Poufności oraz Umowami Przetwarzania Danych Osobowych.
- Dokument powinien zawierać wytyczne dotyczące nadzoru nad przetwarzaniem informacji przez podmioty zewnętrzne oraz obowiązek zgłaszania wszelkich stwierdzonych lub domniemanych nieprawidłowości związanych z przetwarzaniem aktywów.

36. Procedura Dostępu do Sieci i Usług Sieciowych

- Procedura Dostępu do Sieci i Usług Sieciowych musi określać zasady przyznawania dostępu do sieci i usług sieciowych wyłącznie uprawnionym użytkownikom, zgodnie z wymaganiami dotyczącymi identyfikacji, uwierzytelniania i autoryzacji.

- Dokument powinien zawierać wytyczne dotyczące sposobów dostępu, takich jak sieci przewodowe, bezprzewodowe, VPN, oraz połączenia zdalne, a także nadzór nad połączeniami przez Administratora Systemów Informatycznych.

37. Procedura Zarządzania Dostępem Użytkowników

- Procedura Zarządzania Dostępem Użytkowników musi określać zasady rejestrowania, wyrejestrowywania, przydzielania i odbierania praw dostępu użytkownikom systemów informatycznych, zgodnie z upoważnieniami oraz Wnioskami o Nadanie, Zmianę lub Odebranie Dostępu.
- Dokument powinien zawierać wytyczne dotyczące zarządzania prawami uprzywilejowanego dostępu, przeglądów praw dostępu użytkowników oraz bezpiecznego przydzielania poufnych informacji uwierzytelniających.

38. Instrukcja Szyfrowania Informacji w Postaci Cyfrowej z Wykorzystaniem Aplikacji 7-Zip

- Instrukcja musi opisywać proces szyfrowania informacji w postaci cyfrowej przy użyciu aplikacji 7-Zip, w tym instalację oprogramowania oraz procedurę szyfrowania plików z zastosowaniem odpowiednich zabezpieczeń.
- Dokument powinien zawierać wytyczne dotyczące tworzenia bezpiecznych haseł zgodnie z Zasadami Tworzenia i Postępowania z Hasłami oraz sposób odszyfrowania plików przy użyciu właściwego hasła.

39. Polityka Kryptografii

- Polityka Kryptografii musi określać zasady stosowania kryptografii do ochrony poufności, autentyczności i integralności informacji, w tym wymagania dotyczące szyfrowania informacji na nośnikach wymiennych i urządzeniach przenośnych.
- Dokument powinien zawierać wytyczne dotyczące zarządzania kluczami kryptograficznymi, w tym ich generowanie, przechowywanie, archiwizowanie, dystrybucję oraz bezpieczne niszczenie po wycofaniu z użytku.

40. Polityka Bezpieczeństwa Fizycznego i Środowiskowego

- Polityka Bezpieczeństwa Fizycznego i Środowiskowego musi określać zasady zabezpieczania obszarów, w których przetwarzane są informacje, w tym zabezpieczenia wejść, ochronę przed zagrożeniami zewnętrznymi i środowiskowymi oraz kontrolę dostępu do obszarów bezpiecznych.
- Dokument powinien zawierać wytyczne dotyczące ochrony sprzętu, monitorowania warunków środowiskowych, bezpieczeństwa okablowania oraz zasad wynoszenia i zbywania aktywów, w tym stosowanie polityki czystego biurka i czystego ekranu.

41. Polityka Bezpiecznej Eksploatacji

- Polityka Bezpiecznej Eksploatacji musi definiować zasady bezpiecznej eksploatacji systemów informacyjnych, w tym dokumentowanie procedur operacyjnych, zarządzanie zmianami oraz monitorowanie wydajności i pojemności systemów.
- Dokument powinien obejmować wytyczne dotyczące ochrony przed szkodliwym oprogramowaniem, rejestrowania zdarzeń, zarządzania kopią zapasową oraz odpowiedzialności za instalację, konserwację i audyt systemów informacyjnych.

42. Czynności Zabronione

- Dokument "Czynności Zabronione" musi zawierać wykaz działań niedozwolonych w zakresie przetwarzania informacji, takich jak nieujawnianie haseł, niewykorzystywanie nieautoryzowanego oprogramowania oraz obowiązek stosowania polityki czystego biurka i ekranu.
- Dokument powinien określać zasady ochrony urządzeń przed nieuprawnionym dostępem, zakaz używania tego samego hasła w wielu systemach oraz obowiązek szyfrowania chronionych informacji na nośnikach danych i podczas ich przesyłania.

43. Procedura Instalacji i Konfiguracji Systemów Informacyjnych

- Procedura Instalacji i Konfiguracji Systemów Informacyjnych musi definiować zasady instalacji i konfiguracji oprogramowania oraz sprzętu komputerowego przez Administratora Systemów Informatycznych lub inny upoważniony personel, uwzględniając wymagania bezpieczeństwa wynikające z polityk organizacji.
- Dokument powinien zawierać wytyczne dotyczące zarządzania zmianami oprogramowania, utrzymywania poprzednich wersji oraz nadzoru nad dostępem serwisantów dostawców, aby zapobiegać incydentom związanym z bezpieczeństwem informacji.

44. Procedura Konserwacji i Napraw Urządzeń Komputerowych

- Procedura Konserwacji i Napraw Urządzeń Komputerowych musi definiować zasady wykonywania konserwacji i napraw urządzeń komputerowych przez Administratora Systemów Informatycznych lub podmioty zewnętrzne, zgodnie z warunkami określonymi przez producenta.
- Dokument powinien zawierać wytyczne dotyczące nadzoru nad naprawami realizowanymi przez podmioty zewnętrzne oraz obowiązek usunięcia nośników danych lub informacji przed przekazaniem urządzeń do serwisu zewnętrznego.

45. Procedura Obsługi Nośników Informacji

- Procedura Obsługi Nośników Informacji musi określać zasady ochrony nośników informacji przed ich utratą, zniszczeniem, nieuprawnionym odczytem oraz modyfikacją, zarówno dla nośników analogowych, jak i cyfrowych.
- Dokument powinien zawierać wytyczne dotyczące niszczenia uszkodzonych nośników danych, trwałego usuwania informacji przed przekazaniem nośników innym osobom lub podmiotom oraz zgodności z Polityką Zarządzania Aktywami.

46. Procedura Użytkowania Systemów Informacyjnych

- Procedura Użytkowania Systemów Informacyjnych musi definiować zasady korzystania z systemów informacyjnych wyłącznie przez uprawniony personel, zgodnie z przydzielonymi upoważnieniami oraz Polityką Kontroli Dostępu, obejmując autoryzację i uwierzytelnianie.
- Dokument powinien zawierać wytyczne dotyczące odpowiedzialności użytkowników za poufność danych uwierzytelniających, zgłaszanie awarii oraz zgodność użytkowania z warunkami określonymi przez organizację

47. Procedura uruchamiania i Zatrzymania Komputera

- Procedura Uruchamiania i Zatrzymania Komputera musi definiować zasady prawidłowego uruchamiania komputera, w tym sprawdzenie połączeń, włączanie zasilania oraz proces uwierzytelniania użytkownika przy dostępie do systemu operacyjnego.

- Dokument powinien zawierać wytyczne dotyczące bezpiecznego zamykania systemu, odłączania urządzeń przenośnych oraz wyłączania komputera, zabraniając wyłączania poprzez bezpośrednie użycie przycisku zasilania poza sytuacjami awaryjnymi

48. Zasady Tworzenia i Postępowania z Hasłami

- Dokument "Zasady Tworzenia i Postępowania z Hasłami" musi definiować wytyczne dotyczące tworzenia silnych haseł, ich długości (minimum 16 znaków) oraz stosowania wieloskładnikowego uwierzytelniania (MFA) tam, gdzie to możliwe.
- Dokument powinien zawierać zasady poufności haseł, zakaz ich zapisywania w przeglądarkach, wymóg regularnej zmiany haseł co 90 dni oraz zakaz używania tych samych haseł w różnych systemach informatycznych.

49. Polityka Zarządzania Bezpieczeństwem Sieci

- Polityka Zarządzania Bezpieczeństwem Sieci musi definiować zasady ochrony sieci organizacji, w tym zarządzanie urządzeniami sieciowymi, stosowanie zapór sieciowych, monitorowanie oraz uwierzytelnianie dostępu do sieci.
- Dokument powinien zawierać wytyczne dotyczące rozdzielania (segmentacji) sieci, bezpieczeństwa usług sieciowych oraz mechanizmów uwierzytelniania, szyfrowania i ograniczania dostępu do usług, zgodnie z umowami SLA i najlepszymi praktykami.

50. Polityka Przesyłania Informacji

- Polityka Przesyłania Informacji musi definiować zasady ochrony informacji przesyłanych wewnątrz organizacji oraz do podmiotów zewnętrznych, w tym wymóg stosowania ochrony kryptograficznej i zabezpieczeń przed złośliwym oprogramowaniem.
- Dokument powinien zawierać wytyczne dotyczące zawierania porozumień w zakresie przesyłania chronionych informacji, określających środki komunikacji, nadawców, odbiorców oraz mechanizmy ochrony danych.

51. Zasady korzystania z poczty Elektronicznej

- Zasady Korzystania z Poczty Elektronicznej muszą definiować zasady przesyłania informacji chronionych, w tym wymóg stosowania kryptografii i podpisów elektronicznych, gdy wymaga tego prawo lub procedury organizacji.
- Dokument powinien zawierać wytyczne dotyczące korzystania z poczty elektronicznej wyłącznie w celach służbowych, zakaz używania prywatnej poczty elektronicznej na urządzeniach organizacji oraz zasady bezpiecznego postępowania z załącznikami i odnośnikami od nieznanych nadawców.

52. Zasady Korzystania z Internetu

- Zasady Korzystania z Internetu muszą definiować korzystanie z Internetu wyłącznie w celach służbowych, z zakazem pobierania i instalowania nieautoryzowanych plików oraz aplikacji, a także zakazem korzystania z zasobów o treściach przestępczych, pornograficznych lub zakazanych.
- Dokument powinien zawierać wytyczne dotyczące stosowania szyfrowanych połączeń (HTTPS), zakaz używania funkcji autouzupełniania i zapamiętywania haseł w przeglądarkach oraz obowiązek zgłaszania nieprawidłowości do Administratora Systemów Informatycznych.

53. Umowa o Zachowaniu Poufności

- Umowa o Zachowaniu Poufności musi określać zasady ochrony informacji chronionych prawnie, zobowiązując Strony do przetwarzania tych informacji zgodnie z przepisami prawa, wymaganiami regulacyjnymi oraz umownymi, wyłącznie przez upoważniony personel.
- Dokument powinien zawierać wytyczne dotyczące odpowiedzialności za naruszenie poufności, w tym kary umowne i odszkodowania, a także okres obowiązywania zobowiązania do zachowania poufności po zakończeniu realizacji celu umowy.

54. Wymagania Związane z Bezpieczeństwem Systemów Informacji

- Wymagania Związane z Bezpieczeństwem Systemów Informacyjnych muszą obejmować zasady zabezpieczania systemów informacyjnych na każdym etapie ich cyklu życia, w tym identyfikację użytkowników, autoryzację, rejestrowanie działań oraz zarządzanie ryzykiem.
- Dokument powinien zawierać wytyczne dotyczące ochrony usług aplikacyjnych w sieciach publicznych, stosowania kryptografii oraz zabezpieczania transakcji, zapewniając poufność, integralność i dostępność przetwarzanych informacji.

55. Polityka bezpieczeństwa Informacji w Procesach Rozwoju i Wsparcia

- Polityka Bezpieczeństwa w Procesach Rozwoju i Wsparcia musi definiować zasady wprowadzania bezpieczeństwa informacji w całym cyklu życia systemów informacyjnych, w tym podczas prac rozwojowych, testowania i wdrożenia systemów.
- Dokument powinien zawierać wytyczne dotyczące bezpiecznego programowania, zarządzania zmianami w systemach, kontroli wersji oraz testów bezpieczeństwa, zarówno wewnętrznych, jak i zleconych podmiotom zewnętrznym.

56. Wymagania dotyczące Ochrony Danych Testowych

- Wymagania Dotyczące Ochrony Danych Testowych muszą określać zasady doboru, ochrony i nadzoru nad danymi używanymi w procesach testowych, minimalizując użycie rzeczywistych danych osobowych lub chronionych informacji.
- Dokument powinien zawierać wytyczne dotyczące stosowania procedur kontroli dostępu w środowiskach testowych oraz obowiązek usuwania rzeczywistych danych po zakończeniu testów.

57. Polityka Bezpieczeństwa Informacji w Relacjach z Dostawcami

- Polityka Bezpieczeństwa Informacji w Relacjach z Dostawcami musi określać wymagania związane z bezpieczeństwem informacji w relacjach z dostawcami, w tym zobowiązanie do ochrony poufności, integralności i dostępności aktywów organizacji.
- Dokument powinien zawierać wytyczne dotyczące monitorowania i kontroli dostępu dostawców do informacji, zarządzania ryzykiem związanym z łańcuchem dostaw technologii informacyjnych oraz zapewnienia odpowiedniego poziomu bezpieczeństwa w umowach z dostawcami.

58. Zarządzanie Bezpieczeństwem Informacji przez Dostawcę

- Dokument Zarządzanie Bezpieczeństwem Informacji przez Dostawcę musi zawierać szczegółową ankietę oceniającą dostawcę pod kątem zgodności z wymaganiami dotyczącymi bezpieczeństwa informacji, w tym stosowania polityk ochrony danych osobowych, zarządzania ryzykiem oraz incydentami cyberbezpieczeństwa.

- Dokument powinien obejmować pytania dotyczące wdrożenia systemu zarządzania bezpieczeństwem informacji, zarządzania dostępem, szyfrowania oraz przestrzegania zasad „Privacy by design" i „Privacy by default".

59. Procedura zakupu Oprogramowania i Urządzeń Komputerowych oraz Usług IT

- Procedura Zakupu Oprogramowania i Urządzeń Komputerowych oraz Usług IT musi definiować zasady inicjowania, realizacji i weryfikacji zakupów oprogramowania, urządzeń komputerowych oraz usług IT, w tym wymagania dotyczące bezpieczeństwa informacji zgodne z regulacjami prawnymi i wewnętrznymi.
- Dokument powinien zawierać wytyczne dotyczące sporządzania wniosku o zakup, który musi uwzględniać specyfikacje techniczne, planowane zabezpieczenia, potencjalnych dostawców oraz wymagania dotyczące bezpieczeństwa informacji i danych osobowych.

60. Polityka Zarządzania Incydentami, Zdarzeniami, Niezgodnościami i Słabościami

- Polityka Zarządzania Incydentami, Zdarzeniami, Niezgodnościami i Słabościami musi określać zasady postępowania w przypadku incydentów związanych z bezpieczeństwem informacji, w tym ich zgłaszania, oceny, podejmowania decyzji oraz działań zaradczych i korygujących.
- Dokument powinien zawierać wytyczne dotyczące zgłaszania naruszeń danych osobowych do odpowiednich organów w terminie nie dłuższym niż 72 godziny oraz procedury reagowania na incydenty cyberbezpieczeństwa zgodnie z wymogami prawnymi.

61. Zgłoszenie Incydentu, Zdarzenia, Niezgodności, Słabości

- Dokument "Zgłoszenie Incydentu, Zdarzenia, Niezgodności, Słabości" musi umożliwiać zgłaszanie incydentów bezpieczeństwa, zdarzeń, niezgodności z wymaganiami regulacyjnymi oraz słabości w zabezpieczeniach, obejmując opis istoty problemu, aktywów i procesów, których dotyczy.
- Formularz powinien zawierać szczegółowe wytyczne dotyczące dat i okoliczności incydentu, przyczyn jego wystąpienia, rodzaju naruszenia (np. ujawnienie informacji, utrata danych) oraz dane zgłaszającego, świadków i sprawców, umożliwiając anonimowe zgłoszenia.

62. Rejestr Incydentów, Zdarzeń, Niezgodności, Słabości, Działań Zaradczych, Korygujących i Doskonalących

- Rejestr Incydentów, Zdarzeń, Niezgodności, Słabości, Działań Zaradczych, Korygujących i Doskonalących musi zawierać szczegółowy zapis wszystkich incydentów, zdarzeń, niezgodności oraz słabości dotyczących bezpieczeństwa informacji, wraz z datą, opisem problemu oraz podjętymi działaniami.
- Dokument powinien umożliwiać śledzenie działań zaradczych, korygujących i doskonalących, mających na celu poprawę poziomu bezpieczeństwa informacji oraz eliminację zidentyfikowanych problemów.

63. Polityka Ciągłości Bezpieczeństwa Informacji

- Polityka Ciągłości Bezpieczeństwa Informacji musi definiować zasady zapewnienia ciągłości bezpieczeństwa informacji, uwzględniając planowanie, wdrożenie i utrzymanie procesów oraz środków gwarantujących bezpieczeństwo informacji w przypadku zakłóceń, takich jak incydenty czy katastrofy.

- Dokument powinien zawierać wytyczne dotyczące tworzenia planów zarządzania ciągłością działania oraz odtwarzania po katastrofie, weryfikacji zdolności organizacji do zapewnienia ciągłości oraz nadmiarowości zasobów przetwarzania informacji.

64. Ewidencja Aktywów Wspierających Zapewniających Utrzymanie Procesów Krytycznych po Katastrofie

- Ewidencja Aktywów Wspierających Zapewniających Utrzymanie Procesów Krytycznych po Katastrofie musi zawierać identyfikację i szczegółowy opis aktywów niezbędnych do utrzymania ciągłości procesów krytycznych, takich jak pomieszczenia, sprzęt, urządzenia komputerowe, oprogramowanie, nośniki informacji oraz personel.
- Dokument powinien określać minimalne zasoby, w tym powierzchnię, rodzaj sprzętu, liczbę pracowników oraz wymagania dotyczące sieci, niezbędne do realizacji procesów po wystąpieniu katastrofy.

65. Plan Zarządzania Ciągłością Działania

- Plan Zarządzania Ciągłością Działania musi określać zasady postępowania w przypadku zakłóceń procesów krytycznych, w tym procedury odzyskiwania i przywracania działania urządzeń, oprogramowania, sieci, personelu oraz lokalizacji przetwarzania informacji.
- Dokument powinien zawierać wytyczne dotyczące Recovery Time Objective (RTO), Recovery Point Objective (RPO), maksymalnego tolerowanego okresu zakłócenia (MTPD) oraz minimalnego poziomu działalności (MBCO), niezbędnych do zapewnienia ciągłości działania.

66. Plan Zarządzania Odtwarzaniem po Katastrofie

- Plan Zarządzania Odtwarzaniem po Katastrofie musi zawierać zasady przywracania krytycznych procesów organizacji po katastrofie, w tym identyfikację i zabezpieczenie niezbędnych aktywów, takich jak budynki, sprzęt komputerowy, oprogramowanie, nośniki danych oraz personel.
- Dokument powinien określać rodzaje katastrof, takich jak klęski żywiołowe, awarie techniczne, ataki terrorystyczne, oraz procedury reagowania, obejmujące zapewnienie zasobów zastępczych oraz nadzorowanie realizacji planów odtwarzania.

67. Polityka Zgodności

- Polityka Zgodności musi określać zasady monitorowania i przestrzegania wymagań prawnych, regulacyjnych oraz umownych związanych z bezpieczeństwem informacji, w tym ochronę praw własności intelektualnej oraz prywatności danych osobowych.
- Dokument powinien zawierać wytyczne dotyczące regularnych przeglądów zgodności, w tym niezależnych audytów oraz przeglądów technicznych systemów informacyjnych, w celu zapewnienia zgodności z politykami bezpieczeństwa i standardami.

68. Informacje o Przetwarzaniu Danych Osobowych Zbieranych bezpośrednio

- Dokument "Informacje o Przetwarzaniu Danych Osobowych Zbieranych Bezpośrednio" musi określać zasady informowania osób, których dane są przetwarzane, o celach, podstawach prawnych, odbiorcach oraz czasie przechowywania danych osobowych, zgodnie z przepisami RODO.
- Dokument powinien zawierać wytyczne dotyczące praw osób, których dane dotyczą, takich jak prawo do dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu wobec przetwarzania oraz cofnięcia zgody na przetwarzanie danych osobowych.

69. Informacje o Przetwarzaniu Danych Osobowych Zbieranych Pośrednio

- Dokument "Informacje o Przetwarzaniu Danych Osobowych Zbieranych Pośrednio" musi określać zasady informowania osób, których dane zostały pozyskane pośrednio, o celach, podstawach prawnych, odbiorcach oraz czasie przechowywania danych, zgodnie z przepisami RODO.
- Dokument powinien zawierać wytyczne dotyczące praw osób, których dane dotyczą, w tym prawa do dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu oraz cofnięcia zgody na przetwarzanie, a także informacje o zautomatyzowanym podejmowaniu decyzji i profilowaniu.

70. Polityka Ochrony Danych Osobowych

- Polityka Ochrony Danych Osobowych musi definiować zasady przetwarzania danych osobowych zgodnie z wymaganiami prawnymi, regulacyjnymi i umownymi, a także zapewniać ochronę danych identyfikujących osoby fizyczne poprzez odpowiednie środki techniczne i organizacyjne.
- Dokument powinien zawierać wytyczne dotyczące zarządzania danymi, w tym prawa osób, których dane dotyczą, przetwarzanie danych wyłącznie przez upoważniony personel oraz wdrażanie zasad „Privacy by design" i „Privacy by default".

71. Raport z Oceny Skutków Przetwarzania dla Ochrony Danych Osobowych

- Raport z Oceny Skutków Przetwarzania dla Ochrony Danych Osobowych musi zawierać systematyczny opis przetwarzania danych, celów przetwarzania oraz ocenę proporcjonalności i konieczności w stosunku do tych celów, zgodnie z przepisami RODO.
- Dokument powinien zawierać ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, oraz określenie środków planowanych lub zastosowanych w celu zaradzenia tym ryzykom, wraz z ewentualnymi wnioskami dotyczącymi konieczności konsultacji z organem nadzorczym.

72. Rejestr Czynności Przetwarzania Danych Osobowych

- Rejestr Czynności Przetwarzania Danych Osobowych musi zawierać szczegółowe informacje o wszystkich czynnościach przetwarzania danych osobowych, w tym cele przetwarzania, kategorie osób, których dane dotyczą, kategorie danych oraz kategorie odbiorców, którym dane są ujawniane.
- Dokument powinien obejmować opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych w celu ochrony danych osobowych, a także informacje o przekazaniach danych do państw trzecich i planowanych terminach usunięcia danych

73. Rejestr Wszystkich Kategorii czynności Przetwarzania Dokonywanych w Imieniu Administratora

- Rejestr Wszystkich Kategorii Czynności Przetwarzania Dokonywanych w Imieniu Administratora musi zawierać szczegółowy opis wszystkich kategorii czynności przetwarzania realizowanych przez podmiot przetwarzający na rzecz administratora, w tym dane kontaktowe stron oraz kategorie przetwarzanych danych.
- Dokument powinien obejmować informacje o przekazaniach danych do państw trzecich, planowane terminy usunięcia danych oraz opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych w celu ochrony przetwarzanych danych osobowych.

74. Rejestr Zbiorów Danych Osobowych

- Rejestr Zbiorów Danych Osobowych musi zawierać identyfikację wszystkich zbiorów danych osobowych przetwarzanych przez organizację, w tym ich nazwy, cele przetwarzania oraz czynności przetwarzania realizowane w ramach każdego procesu.
- Dokument powinien zawierać informacje o administratorze danych, identyfikatory zbiorów oraz procesy związane z przetwarzaniem danych, zapewniając pełną ewidencję przetwarzanych danych osobowych w organizacji.

75. Test Równowagi

- Test Równowagi musi zawierać ocenę prawnie uzasadnionych interesów realizowanych przez administratora w odniesieniu do interesów, podstawowych praw i wolności osób, których dane dotyczą, w celu ustalenia, czy przetwarzanie danych osobowych na tej podstawie jest zgodne z RODO.
- Dokument powinien uwzględniać analizę korzyści i ryzyk związanych z przetwarzaniem, w tym ocenę możliwości naruszenia prywatności, anonimowości oraz innych praw osób, których dane dotyczą, aby zdecydować o zastosowaniu prawnie uzasadnionego interesu jako podstawy prawnej przetwarzania.

76. Umowa Przetwarzania Danych Osobowych w Imieniu Administratora

- Umowa Przetwarzania Danych Osobowych w Imieniu Administratora musi określać zasady przetwarzania danych osobowych przez podmiot przetwarzający, zgodnie z wytycznymi administratora, w tym cel przetwarzania, rodzaje danych oraz kategorie osób, których dane dotyczą.
- Dokument powinien zawierać wytyczne dotyczące obowiązków obu stron, w tym wymogi dotyczące bezpieczeństwa, obowiązek raportowania naruszeń oraz możliwość audytu zgodności z przepisami o ochronie danych osobowych.

77. Zawiadomienia Osoby, Której Dane Dotyczą o Naruszeniu Ochrony Danych Osobowych

- Zawiadomienie Osoby, Której Dane Dotyczą, o Naruszeniu Ochrony Danych Osobowych musi informować osobę o charakterze naruszenia, możliwych konsekwencjach dla niej oraz środkach zastosowanych przez administratora w celu zaradzenia skutkom naruszenia, zgodnie z art. 34 RODO.
- Dokument powinien zawierać szczegółowy opis incydentu, obejmujący datę, czas, okoliczności, kategorie dotkniętych danych oraz zalecenia dla osoby, której dane dotyczą, w celu zminimalizowania negatywnych skutków naruszenia.

78. Wycofanie Zgody na Przetwarzanie Danych Osobowych

- Dokument "Wycofanie Zgody na Przetwarzanie Danych Osobowych" musi umożliwiać osobom wycofanie zgody na przetwarzanie ich danych osobowych, zgodnie z art. 7 RODO, poprzez złożenie odpowiedniego wniosku zawierającego dane osoby oraz zakres wycofanej zgody.
- Dokument powinien zawierać sekcje umożliwiające określenie rodzaju danych, których przetwarzanie zostaje wycofane, oraz cele przetwarzania, z których osoba chce wycofać swoją zgodę

79. Zgoda na Przetwarzanie Danych Osobowych

- Dokument "Zgoda na Przetwarzanie Danych Osobowych" musi umożliwiać osobie wyrażenie dobrowolnej i świadomej zgody na przetwarzanie jej danych osobowych, zgodnie z art. 6 RODO, z wyszczególnieniem rodzajów danych oraz celów ich przetwarzania.

- Dokument powinien zawierać informację o prawie osoby do wycofania zgody w dowolnym momencie, bez wpływu na zgodność z prawem wcześniejszego przetwarzania, oraz o łatwości wycofania zgody na równi z jej wyrażeniem.

Część 4

1. Szkolenie z cyberbezpieczeństwa dla kadry administracyjnej.

Szkolenie dla pracowników administracyjnych w zakresie cyberbezpieczeństwa
Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników administracyjnych.
Szkolenie stacjonarne lub online z zakresu cyberbezpieczeństwa skierowane do pracowników administracyjnych, obejmujące co najmniej następujące obszary:

a. wprowadzenie do cyberbezpieczeństwa:
   - czym jest cyberbezpieczeństwo;
   - dlaczego cyberbezpieczeństwo jest ważne;
   - kluczowe zagadnienia związane z cyberbezpieczeństwem;
   - przegląd statystyk i trendów w cyberbezpieczeństwie.

b. typy zagrożeń w cyberprzestrzeni:
   - malware (wirusy, trojany, robaki itp.);
   - ataki typu phishing i spear phishing;
   - ataki DDoS;
   - ataki ransomware;
   - zagrożenia związane z sieciami społecznościowymi.

c. zasady bezpieczeństwa i praktyki:
   - zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
   - zasady bezpieczeństwa e-mail;
   - bezpieczeństwo w sieciach bezprzewodowych;
   - bezpieczne przeglądanie internetu;
   - backup i odzyskiwanie danych.

d. reagowanie na incydenty i planowanie awaryjne:
   - jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
   - zasady reagowania na incydenty;
   - planowanie awaryjne i kontynuacja działalności;
   - Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

Przewiduje się, że szkolenie potrwa łącznie minimum 16 godzin roboczych, rozłożonych na co najmniej 2 dni. Zajęcia będą organizowane w grupach szkoleniowych, gdzie każda grupa będzie miała 4 godziny zajęć dziennie. Dodatkowo, każda sesja będzie obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

2. Szkolenie z cyberbezpieczeństwa dla kadry informatycznej.

Szkolenie dla pracowników IT w zakresie cyberbezpieczeństwa
Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa:
Szkolenie z cyberbezpieczeństwa dla pracowników IT.
Indywidualne warsztaty online z zakresu cyberbezpieczeństwa skierowane do administratorów sieci teleinformatycznej, obejmujące co najmniej następujące obszary:

1. Wprowadzenie do cyberbezpieczeństwa:
   - Czym jest cyberbezpieczeństwo?
   - Dlaczego cyberbezpieczeństwo jest ważne?
   - Kluczowe zagadnienia związane z cyberbezpieczeństwem.
   - Przegląd statystyk i trendów w cyberbezpieczeństwie.
2. Typy zagrożeń w cyberprzestrzeni:
   - Malware (wirusy, trojany, robaki itp.)
   - Ataki typu phishing i spear phishing
   - Ataki DDoS
   - Ataki ransomware
   - Zagrożenia związane z sieciami społecznościowymi.
3. Zasady bezpieczeństwa i praktyki:
   - Zarządzanie hasłami i uwierzytelnianie wieloskładnikowe
   - Zasady bezpieczeństwa e-mail
   - Bezpieczeństwo w sieciach bezprzewodowych
   - Bezpieczne przeglądanie internetu
   - Backup i odzyskiwanie danych
4. Bezpieczeństwo systemów i sieci
   - Zasady bezpieczeństwa systemów operacyjnych
   - Bezpieczeństwo sieci i firewall
   - Wprowadzenie do VPN
   - Bezpieczeństwo urządzeń IoT
   - Bezpieczeństwo w chmurze
5. Reagowanie na incydenty i planowanie awaryjne
   - Jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem
   - Zasady reagowania na incydenty
   - Planowanie awaryjne i kontynuacja działalności
   - Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione
6. Aktualne trendy i przyszłość cyberbezpieczeństwa
   - Sztuczna inteligencja i machine learning w cyberbezpieczeństwie
   - Kryptografia i blockchain
   - Bezpieczeństwo danych w erze Big Data
   - Przyszłość cyberbezpieczeństwa: wyzwania i możliwości

Przewiduje się, że szkolenie potrwa łącznie minimum 8 godzin roboczych, rozłożonych na co najmniej 1 dzień. Zajęcia będą organizowane w grupach szkoleniowych, gdzie każda grupa będzie miała 4 godziny zajęć dziennie. Dodatkowo, każda sesja będzie obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

3. Szkolenie specjalistyczne dla kadry zarządzającej.

Zaawansowane Szkolenie z Cyberbezpieczeństwa dla Kadry Zarządzającej

Cel szkolenia:
Przekazanie menedżerom zaawansowanej wiedzy i narzędzi niezbędnych do efektywnej ochrony przed rosnącymi zagrożeniami cybernetycznymi, poprzez pogłębione rozumienie ryzyk, strategii obronnych, regulacji prawnych oraz najnowszych trendów w cyberbezpieczeństwie.

Struktura programu szkoleniowego:
Szkolenie powinno być kompleksowym procesem, który umożliwia uczestnikom zdobycie dogłębnej wiedzy na temat wybranych zagadnień. Powinno ono nie tylko dostarczyć podstawowej informacji, ale także omówić zaawansowane aspekty danej tematyki, aby uczestnicy mieli pełniejsze zrozumienie tematu i byli w stanie zastosować zdobytą wiedzę w praktyce. Przekazywanie wiedzy powinno być interaktywne i angażujące, wykorzystując różnorodne metody nauczania, takie jak prezentacje, dyskusje, studia przypadków czy praktyczne ćwiczenia, co pozwoli uczestnikom efektywniej przyswoić omawiany materiał.

W ramach przeprowadzonego szkolenia wykonawca

1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:
- Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.
- Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskają wgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatak może mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.

2. Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji:
- Normy ISO/IEC: Szczegółowe omówienie serii norm: ISO/IEC 27000: (zarysowuje leksykon oraz globalne zasady nadrzędne systemu zarządzania bezpieczeństwem informacji, kreśląc fundament pod szersze zrozumienie oraz efektywniejsze stosowanie pozostałych norm z rodziny 27000), ISO/IEC 27001 (stanowi kanon dotyczący wymagań dla systemów zarządzania bezpieczeństwem informacji, umożliwiając organizacjom zabezpieczenie informacji pod kątem ich poufności, integralności oraz dostępności przez implementację adekwatnych procedur zarządczych), ISO/IEC 27002 (oferuje referencyjny zbiór praktyk dla organizacji dążących do identyfikacji, wdrażania, utrzymania oraz doskonalenia swoich mechanizmów ochrony informacji w kontekście SZBI), ISO/IEC 27004 (dostarcza metodykę do monitorowania, przeglądu, oceny oraz doskonalenia efektywności systemu zarządzania bezpieczeństwem informacji, akcentując znaczenie mierzalnych wskaźników), ISO/IEC 27005 (zawiera wytyczne dotyczące zarządzania ryzykiem w kontekście bezpieczeństwa informacji, nakreślając proces identyfikacji, oceny oraz zarządzania ryzykiem informacyjnym), ISO/IEC 27006 (określa wymogi dla organizacji świadczących usługi certyfikacji systemów zarządzania bezpieczeństwem informacji, wyznaczając ramy dla procesu audytu i certyfikacji), ISO/IEC 27013 (podaje wytyczne integrujące system zarządzania bezpieczeństwem informacji z systemem zarządzania usługami IT, promując koherentną i efektywną infrastrukturę zarządzania), ISO/IEC 27017 (koncentruje się na bezpieczeństwie informacji w chmurze, proponując kontrole oraz wytyczne dla dostawców i użytkowników usług przetwarzania w chmurze), ISO/IEC 27018 (ustanawia kodeks praktyk dla ochrony informacji osobowych w chmurze, zgodnie z wymaganiami prywatności i ochrony danych), ISO/IEC 22301 (specyfikuje wymogi dla systemów zarządzania ciągłością działania, umożliwiając organizacjom przygotowanie na incydenty zakłócające normalne funkcjonowanie), ISO/IEC 24762 (zawiera wytyczne dla usług odzyskiwania po awariach w centrach danych i innych środowiskach IT, podkreślając kluczowe elementy potrzebne do przywrócenia operacji IT po katastrofie, ISO/IEC 27036 (skupia się na zarządzaniu bezpieczeństwem informacji w relacjach między organizacjami, oferując wytyczne dotyczące bezpieczeństwa w outsourcingu i partnerstwach biznesowych), ISO/IEC 31000 (dostarcza wytyczne dotyczące zarządzania ryzykiem ogólnym, promując model zarządzania ryzykiem, który można dostosować do różnych typów organizacji i kontekstów), 13501-2 (norma ta przeprowadza proces kategoryzacji reakcji na ogień wyrobów używanych w budownictwie oraz elementów konstrukcyjnych budowli, określając ich parametry odporności na pożary i zachowanie w ekstremalnych warunkach termicznych), norma 1627 (stanowi kryteria odporne na nieautoryzowany dostęp przez systemy zamykające, jak okna, drzwi oraz osłony, hierarchizując je zgodnie z ich zdolnością do stawiania oporu przy próbach sforsowania), norma 12209-04 (wytycza wymagania techniczne oraz procedury badawcze dla mechanizmów blokujących w obszarze budowlanym, takich jak zamki mechaniczne wraz z ich komponentami, oceniając ich funkcjonalność oraz

niezawodność.), norma 50131-1 (określa specyfikacje dla systemów alarmowych przeznaczonych do sygnalizacji prób włamania czy napadu, wyznaczając standardy dotyczące ich skuteczności oraz metodyki testowania).

- Omówienie znaczenia powyższych norm i ich w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.
- Inne standardy: Przedstawienie i dyskusja na temat innych standardów:
    - ramy dotyczące zarządzania ryzykiem cyberbezpieczeństwa - NIST Cybersecurity Framework;
    - ramy dotyczące wdrażania, rozwoju i doskonalenia polityki IT – COBIT;
    - zbiór praktyk dotyczący zarządzania usługami IT – ITIL;
    - akceptowalna polityka szyfrowania SANS;
    - techniki kryptograficzne - ENISA ;
    - ramy ochrony informacji i zasobów federalnych agencji rządowych USA - 800-53 rev3.
- Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.

3. Omówienie zaawansowanych strategii ochrony organizacji:

- Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.
- Wprowadzenie do zarządzania incydentami, zdefiniowanie incydentów i wektorów ataku: atak przeprowadzony z nośnika wymiennego lub urządzenia peryferyjnego, atak wykorzystujący metody brute-force w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług, ataki wykonane z poziomu witryny internetowej lub aplikacji internetowej, atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika, naruszenia zasad dopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych kategorii, utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, na przykład laptopa lub urządzenia typu smartfon.
- Szczegółowy opis i kroki zarządzania incydentami:
    - wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
    - rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;
    - analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;
    - klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.
    - priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje z możliwymi konsekwencjami incydentu dla misji instytucji;
    - podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;
    - ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.
- Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:
    - **Priorytet krytyczny** - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
    - **Priorytet wysoki** - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
    - **Priorytet średni** - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.
- Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.

- Lista omówionych kompetencji w szkoleniu:
    - Szef działu bezpieczeństwa (kierownik, dyrektor);
    - Pełnomocnik ds. Bezpieczeństwa Informacji;
    - Specjalista ds. Zarządzania Ryzykiem;
    - Specjalista ds. Zgodności;
    - Specjalista ds. Bezpieczeństwa Fizycznego;
    - Architekt Systemów Bezpieczeństwa;
    - Koordynator Programu Bezpieczeństwa;
    - Analityk Bezpieczeństwa (II linia wsparcia);
    - Inżynier ds. Bezpieczeństwa (II linia wsparcia);
    - Administrator Systemów Bezpieczeństwa (II linia wsparcia);
    - Specjalista ds. Odpowiedzi na Incydenty (III linia wsparcia);
    - Specjalista ds. Testów Penetracyjnych (III linia wsparcia);
    - Specjalista ds. Testów Socjotechnicznych (III linia wsparcia).

4. Regulacje prawne i compliance:
- Zharmonizowanie działalności Podmiotu z imperatywami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, z naciskiem na implementację procedur i protokołów zapewniających wytrzymałość infrastruktury informatycznej na potencjalne zagrożenia cyfrowe.
- Inicjacja, adaptacja, perpetuacja oraz ewolucja Systemu Zarządzania Bezpieczeństwem Informacji, skonstruowanego na fundamencie czterech norm określonych w paragrafie 20 Krajowego Ramienia Interoperacyjności, stanowiących kamień węgielny dla ochrony danych.
- Egzekwowanie procedury tworzenia redundancji danych dziennikowych poprzez generowanie kopii zapasowych, które będą przechowywane przez okres minimalny dwóch lat, zgodnie z dyrektywą zawartą w paragrafie 21 Krajowego Ramienia Interoperacyjności.
- Implementacja kompleksowej agregacji logów (rejestrowanych zdarzeń) pochodzących z heterogenicznej gamy urządzeń, maszyn i aplikacji działających w ramach infrastruktury teleinformatycznej Podmiotu, umożliwiająca szczegółową analizę i audyt bezpieczeństwa.
- Integracja z zaawansowanym systemem zarządzania cyberbezpieczeństwem S46 (S46-react), celem optymalizacji procesów detekcji, reagowania i prewencji w zakresie incydentów bezpieczeństwa cyfrowego.
- Kodyfikacja programu regularnych audytów wewnętrznych i zewnętrznych, obejmujących spektrum standardów i regulacji (KRI, KSC, ISO, RODO), wraz z przeprowadzaniem testów penetracyjnych i socjotechnicznych, mających na celu weryfikację skuteczności implementowanych środków ochrony.
- Monitorowanie zdarzeń systemowych w trybie ciągłym, poprzez wykorzystanie mechanizmów korelacji zdarzeń, umożliwiających identyfikację i interpretację wzorców aktywności sugerujących potencjalne scenariusze ataków cybernetycznych.
- Dostosowanie się do rozszerzonego zakresu wymagań wynikających z implementacji Dyrektywy NIS2, która wprowadza nowe, zaostrzone standardy w zakresie cyberbezpieczeństwa, wymagające od organizacji ponownej oceny i ulepszenia istniejących strategii ochrony danych.
- Wyznaczenie dedykowanego Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, którego rola nie będzie interferować ani generować konfliktów interesów z innymi kluczowymi funkcjami w organizacji (np. Inspektorem Ochrony Danych, Informatykiem, Dyrektorem).
- Rekonfiguracja systemów informatycznych oraz protokołów pracy zdalnej w zgodzie ze zmienionymi standardami bezpieczeństwa, uwzględniającymi nowelizację Kodeksu Pracy, w celu zabezpieczenia integralności danych korporacyjnych w rozproszonym środowisku pracy.
- Realizacja oczekiwań organów nadzorczych w kontekście konstruowania oraz utrzymywania zaawansowanych systemów cyberbezpieczeństwa, zdolnych do przeciwdziałania współczesnym zagrożeniom w przestrzeni cyfrowej.
- Implementacja rygorystycznych protokołów ochrony danych osobowych, mających na celu eliminację ryzyka wycieków informacji, spowodowanych przez nieświadome bądź intencjonalne działania personelu organizacji.
- Automatyzacja procesów aktualizacji oprogramowania w celu zapewnienia najwyższego poziom

5. Zarządzanie bezpieczeństwem w praktyce:
- Zrozumienie znaczenia typów licencji względem konieczności ich testowania:
    - Licencje niewyłączne, w których udzielający licencji może zezwolić na korzystanie z utworu wielu osobom równocześnie, które nie muszą mieć formy pisemnej.

- Licencje wyłączne, spotykane głównie w przypadku oprogramowania pisanego na zamówienie (np. strona www), w tym przypadku zwykle umowa licencyjna wynika z umowy o dzieło, na podstawie której firma wykonująca oprogramowanie wykonuje zamówioną aplikację, umowa taka wymaga formy pisemnej pod rygorem nieważności.
- Sublicencja, w której licencjobiorca może udzielić dalszej licencji, pod warunkiem wszakże takiego upoważnienia w jego umowie licencyjnej.
- OEM, to programy sprzedawane wraz ze sprzętem komputerowym (przypisane do konkretnego komputera), po wymianie sprzętu na nowszy, nie można ich przenieść na nowy komputer tylko trzeba ponownie je zakupić.
- BOX, to programy, które można przenosić na kolejne komputery jednak pod warunkiem, że zawsze zainstalowany jest tylko na jednym komputerze. Legalny jest tylko program ostatnio zainstalowany.
- Open Source (otwarte oprogramowanie) to alternatywa dla Freeware (wolne oprogramowanie), którego celem jest istnienie swobodnego dostępu do oprogramowania dla wszystkich jego uczestników. Zapewnia swoim użytkownikom prawo do legalnego oraz darmowe.

- Techniki hardeningu: Wzmocnienie infrastruktury IT oraz zarządzanie patchami bezpieczeństwa.
- Testy penetracyjne i socjotechniczne: Organizacja i przeprowadzanie testów w celu oceny gotowości organizacji

Szkolenie powinno odbyć się w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem co najmniej 4 przerw po 15 minut. Powinno jest 30 minut na pytania i odpowiedzi uczestników.

4. Szkolenie specjalistyczne dla informatyków.

Szkolenie z obsługi oprogramowania przeciwdziałającego wyciekowi danych
Przedmiotem zamówienia jest przeprowadzenie szkolenia stacjonarnego lub online dla personelu IT, w celu przekazania kompletnej wiedzy w zakresie obsługi i wykorzystania funkcji oprogramowania przeciwdziałającego wyciekowi danych, w ich codziennej pracy.
Szkolenie obejmie co najmniej następujące obszary:

- Podstawowe informacje
- Licencjonowanie
- Wspierane systemy operacyjne
- Wdrożenie oprogramowania przeciwdziałającego wyciekowi danych
- Omówienie instalatora oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie serwera oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie agentów oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie klientów oprogramowania przeciwdziałającego wyciekowi danych
- Uruchomienie modułu analitycznego
- Analiza wycieków danych
- Filtrowanie i raporty z analizy
- Uruchomienie modułu przeciwdziałającego wyciekowi danych
- Uruchomienie szyfrowania BitLockerem
- Konfiguracja dostępu do urządzeń i portów
- Interfejs webowy oprogramowania przeciwdziałającego wyciekowi danych
- Minimalne wymagania systemowe dla omawianego oprogramowania
- Instalacja oraz konfiguracja modułu webowego oprogramowania przeciwdziałającego wyciekowi danych
- Analiza zachowań
- Zarządzenie kategoriami produktywności
- Kontrola WWW i aplikacji
- Alerty, raporty i konserwacja
- Zaawansowane DLP dla oprogramowania przeciwdziałającego wyciekowi danych
- Reguły DLP – tryby polityk
- Reguły ogólne
- Reguły aplikacji
- Po co nam kategorie danych?

- Inteligentne wyszukiwanie danych osobowych
- Czym są tagi i do czego służą?
- Reguły tagowania dla aplikacji, stron oraz lokalizacji

5. Szkolenie AD / wirtualizacja / kopie zapasowe

1. Szkolenie z zakresu Active Directory (AD):
Inicjatywa szkoleniowa dedykowana Active Directory ma za zadanie zapewnić uczestnikom wszechstronne przygotowanie do efektywnego zarządzania oraz ochrony infrastruktury Active Directory, stanowiąc fundament dla bezpiecznego i zrównoważonego zarządzania tożsamościami i dostępami w sieciowych ekosystemach organizacyjnych. Program szkoleniowy został skonstruowany tak, aby objąć spektrum zagadnień, począwszy od elementarnych, aż po zaawansowane moduły:
- Ekspozycja na Architekturę Active Directory: Wstępna faza szkolenia skupia się na dogłębnym zarysie roli i kardynalnego znaczenia infrastruktury Active Directory w procesach zarządzania identyfikowalnością użytkowników oraz moderacji dostępu. Uczestnicy zostaną wprowadzeni w kompleksową architekturę AD, eksplorując jej kluczowe usługi i funkcjonalności, w tym mechanizmy uwierzytelniania, autoryzacji oraz efektywne zarządzanie zasobami.
- Podstawy Konfiguracji i Administracji Obiektami w AD: Moduł ten kładzie nacisk na praktyczne aspekty tworzenia, konfiguracji i zarządzania obiektami takimi jak użytkownicy, grupy i komputery, działającymi w obrębie środowiska AD. Uczestnicy zdobędą umiejętności w zakresie procedur dodawania, usuwania i modyfikacji obiektów, korzystając z dedykowanych narzędzi administracyjnych.
- Wprowadzenie do Mechanizmów Polityk Grupowych: Szczegółowe omówienie i analiza roli polityk grup (Group Policy) w kontekście zarządzania konfiguracją i bezpieczeństwem infrastruktury AD. Szkolenie obejmuje metodyki tworzenia, aplikacji i administrowania politykami grupowymi, ukazując ich wpływ na regulacje i konfiguracje zarówno klientów, jak i serwerów w domenie.
- Implementacja Zasad Bezpieczeństwa w AD: Dyskusja na temat strategii i metodologii wzmocnienia zabezpieczeń infrastruktury AD, obejmująca zarządzanie uprawnieniami, monitorowanie aktywności w logach oraz konfigurację polityk bezpieczeństwa. Szkolenie podkreśla praktyczne podejście do identyfikacji, reagowania oraz efektywnego rozwiązywania incydentów bezpieczeństwa.
- Strategie Ochrony AD Przed Atakami: Analiza potencjalnych zagrożeń dla infrastruktury AD oraz zapewnienie szkolenia z procedur szybkiego reagowania i odtwarzania funkcjonalności systemu w przypadku wystąpienia ataków lub innych awarii. Ten segment szkolenia jest poświęcony rozwijaniu kompetencji w zakresie przeciwdziałania zagrożeniom, przywracania systemu do stanu operacyjnego oraz zapewnienia ciągłości działania krytycznych usług.

2. Szkolenie z zakresu zabezpieczeń wirtualizacji:
Inicjatywa ta jest skoncentrowana na intensyfikacji świadomości oraz ekspansji umiejętności technicznych związanych z aspektami bezpieczeństwa operacyjnego w środowiskach wirtualizowanych. Program szkoleniowy został zaprojektowany tak, aby oferować kompendium wiedzy obejmujące kluczowe segmenty:
- Fundamenty Technologii Wirtualizacji: Wstępna część szkolenia dedykowana jest dogłębnemu zrozumieniu essencji technologii wirtualizacji, przybliżając uczestnikom szeroki wachlarz platform wirtualizacyjnych, w tym, lecz nie ograniczając się do, Vmware oraz Hyper-V. Uczestnicy zostaną zaznajomieni z kluczowymi funkcjami, możliwościami oraz praktycznymi zastosowaniami tych technologii w różnorodnych kontekstach biznesowych, uwydatniając ich strategiczne znaczenie dla nowoczesnych przedsiębiorstw.
- Konstrukcja, Konfiguracja i Administrowanie Maszynami Wirtualnymi: Ten moduł szkolenia skupia się na przekazaniu praktycznych wskazówek dotyczących procesów kreowania, konfiguracji oraz zarządzania wirtualnymi maszynami. Szczególny nacisk kładziony jest na procedury instalacji systemów operacyjnych, alokacji zasobów oraz konfiguracji komunikacji sieciowej, z zamiarem maksymalizacji efektywności i wydajności wirtualnych środowisk operacyjnych.
- Metodologie Ochrony Infrastruktury Wirtualizowanej: Zaawansowany segment szkolenia poświęcony jest szczegółowej analizie i implementacji technik zabezpieczających infrastrukturę wirtualizowaną. Uczestnicy zgłębią metody i narzędzia umożliwiające izolację maszyn wirtualnych, zabezpieczanie hypervisorów oraz zarządzanie sieciami wirtualnymi, z naciskiem na kluczowe procedury monitorowania zagrożeń, konfigurację zasad zapór sieciowych oraz techniki segmentacji sieci wirtualnych. Omówione zostaną również zaawansowane strategie ochrony przed złośliwym oprogramowaniem i atakami sieciowymi, mające na celu zwiększenie odporności i bezpieczeństwa całego ekosystemu wirtualnego.

3. Szkolenie z zakresu bezpieczeństwa kopii zapasowych:

Inicjatywa szkoleniowa skoncentrowana na bezpieczeństwie kopii zapasowych kieruje się ku dogłębnemu zrozumieniu i praktycznej maestrii w zakresie kreowania oraz administracji bezpiecznymi mechanizmami backupu danych, akcentując na kluczowych komponentach:
- Fundamenty Backupu i Jego Znaczenie w Kontekście Bezpieczeństwa IT: Inauguracyjny moduł kursu dokonuje eksplikacji kluczowych pojęć i terminologii związanej z procesem tworzenia kopii zapasowych, podkreślając ich nieodzowną rolę w kompleksowej strategii bezpieczeństwa technologii informacyjnych oraz w zapewnieniu nieprzerwanej operacyjności korporacyjnych ekosystemów. Uczestnicy zdobywają perspektywę na istotę backupów jako niezbędnej linii obrony przed incydentami, które mogą zagrozić ciągłości działania organizacji.
- Dogłębna Analiza Typologii Kopii Zapasowych: Kurs prowadzi przez szczegółowe wyjaśnienie różnorodności form backupów – od pełnych, przez przyrostowe, aż po różnicowe – oferując równocześnie pragmatyczne wytyczne dotyczące ich efektywnego planowania, konfiguracji i implementacji. Omówienie to jest kluczowe dla zrozumienia optymalnych metod zarządzania cyklem życia danych oraz dla maksymalizacji efektywności procesów backupu.
- Implementacja Nowoczesnych Rozwiązań Backupowych: Ten segment szkolenia koncentruje się na adaptacji oraz wykorzystaniu zaawansowanych technologii i oprogramowania backupowego, włączając w to systemy lokalne oraz oparte na chmurze, techniki deduplikacji danych, mechanizmy kompresji oraz szyfrowania. Przedstawione zostają najnowsze narzędzia i metodologie, które umożliwiają zwiększenie efektywności i bezpieczeństwa procesów archiwizacji danych.
- Weryfikacja Efektywności Backupu i Strategii Odtwarzania: Kurs zawiera kompleksowe instrukcje dotyczące testowania efektywności tworzonych kopii zapasowych oraz procedur przywracania danych, z naciskiem na strategie prewencji i reagowania na kryzysy takie jak ataki ransomware. Uczestnicy uzyskują wiedzę na temat kluczowych praktyk i procedur testowych, które zapewniają gotowość na scenariusze awaryjne.
- Procedury i Strategie Odzyskiwania Danych po Awarii: Finalny moduł edukacyjny zagłębia się w omówienie metodyk i praktycznych wytycznych szybkiego odzyskiwania funkcjonalności systemów po wystąpieniu incydentów. Szczególna uwaga poświęcona jest skutecznym strategiom odzyskiwania danych, które są fundamentem dla minimalizacji czasu przestoju i optymalizacji procesu odbudowy po awarii.

Cel szkolenia:
Podstawowym zamierzeniem niniejszego kursu szkoleniowego jest dostarczenie uczestnikom kompleksowego zestawu wiedzy teoretycznej oraz praktycznych kompetencji, które są krytyczne dla skutecznego administrowania i nadzorowania bezpieczeństwem infrastruktury technologicznej informacyjnej. Szczególny nacisk kładziony jest na głębokie zrozumienie i zarządzanie systemem Active Directory, ekosystemami wirtualizacji oraz złożonymi strategiami implementacji systemów kopii zapasowych. Celem tego szkolenia jest nie tylko przekroczenie granic czysto teoretycznego przekazu wiedzy, ale przede wszystkim rozwinięcie praktycznych umiejętności aplikacyjnych, które umożliwią uczestnikom efektywne zabezpieczanie wartościowych zasobów informatycznych przed rosnącą gamą zagrożeń cyfrowych oraz zagwarantowanie nieprzerwanej operacyjności systemów informatycznych.
Poprzez syntezę teoretycznych fundamentów z realnymi aplikacjami praktycznymi, program ma na celu wyekwipowanie uczestników w niezbędne narzędzia do identyfikacji, adekwatnej reakcji oraz neutralizacji potencjalnych zagrożeń bezpieczeństwa cyfrowego. Ponadto, kurs stawia za cel wdrożenie uczestników w głębinę najlepszych praktyk i standardów branżowych, które stanowią o kształcie profesjonalnej codziennej praktyki. Skupienie się na tych elementach ma kluczowe znaczenie dla kształtowania w uczestnikach umiejętności nie tylko reaktywnych, ale przede wszystkim proaktywnych w kontekście zarządzania ryzykiem i ochrony infrastruktury IT. W rezultacie, program szkoleniowy ma na celu przygotowanie adeptów do pełnienia roli bastionu w obronie przed zagrożeniami, promując jednocześnie kulturę bezpieczeństwa informacyjnego, która jest fundamentem dla zrównoważonego rozwoju i innowacyjności w przestrzeni technologicznej organizacji.

Część 5

1. **Agregat – 1 sztuka.**

Poniżej przedstawiono szczegółowe wymagania dla agregatu prądotwórczego.

Agregat prądotwórczy ma być wykonany w obudowie zewnętrznej wyciszonej, panelowej umożliwiająca modyfikacje agregatu lub konwersję na urządzenie otwarte pokrytą proszkowo farbą epoksydową.
Solidna konstrukcja, która zapewnia łatwy dostęp do połączeń oraz części podczas przeglądów okresowych.

Dane wymiarowe:

Długość (L) mm 2200
Szerokość (W) mm 1020
Wysokość (H) mm 1292
Waga suchy (kg) 866 kg

Poziom hałasu

Poziom ciśnienia akustycznego z @ 1 m 75 dBA
Poziom ciśnienia akustycznego z @ 7 m 63 dBA

Agregat powinien być wyposażony w nowoczesny panel kontroli ze sterowaniem mikroprocesorowym z możliwością programowania podstawowych parametrów pracy.

Panel sterowania powinien być zabezpieczony zamykanymi drzwiami z przeszklonym wizjerem.
Agregat ma być wyposażony w nowoczesny silnik wysokoprężny zapewniający dobrą stabilizację częstotliwości i diagnostykę oraz w główne zabezpieczenie – wyłącznik kompaktowy.
W ramach dostawy zawarte mają być:

a) dostawa agregatu w obudowie zewnętrznej o podanych parametrach na miejsce instalacji
a) przeszkolenie obsługi pod względem prawidłowej eksploatacji
b) pełna dokumentacja agregatu
c) Próby pracy agregatu podłączonego do zasilania budynku
d) Gwarancja producenta agregatu: 60 miesięcy z limitem 1000 mth.
e) producent agregatu posiadający certyfikaty ISO9001 i ISO14001 potwierdzone dokumentem.
f) dostawca musi posiadać autoryzację do obsługi serwisowej silnika oraz prądnicy (ASO – Autoryzowana Stacja Obsługi)
g) obecność Producenta marki na rynku w Polsce powyżej 10 lat (sprzedaż, serwis, magazyn części)
h) Zamawiający wymaga przed przystąpieniem do złożenia oferty oględzin miejsca przyłącza agregatu, z zastrzeżeniem, że oględziny mogą być wykonane w formie ustalonej z zamawiającym – w przeciwnym wypadku oferta podlega odrzuceniu.

Oferowane urządzenia (dotyczy silnika i prądnicy oraz całego agregatu) są fabrycznie nowe, bez śladu użytkowania i posiadają stosowny pakiet usług gwarancyjnych kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej, pochodzą z oficjalnego, autoryzowanego kanału sprzedaży na rynek polski, posiadają serwis i wparcie producenta.

Główne parametry agregatu .

- Moc maksymalna ESP kVA min – 45.0
- Moc maksymalna ESP kW min – 36.0

- Moc znamionowa PRP kVA min - 41.3
- Moc znamionowa PRP kW min – 33.0
- Napięcie V 400/230
- Częstotliwość Hz 50
- Współczynnik mocy cos φ 0.8
- Liczba faz 3
- Paliwo Diesel

Prądnica:

- Uzwojenie Standardowe
- Połączenie uzwojenia Typ Gwiazda
- Częstotliwość Hz 50
- Napięcie V 400
- Liczba faz 3
- Współczynnik mocy cos φ 0.8
- Moc awaryjna kVA 49.5
- Nominalna moc ciągła kVA 45.0
- Sprawność @ 100% % - 87.6
- Typ Bez szczotkowy
- Bieguny 4 Tolerancja napięcia % 1
- Klasa izolacji H
- Klasa IP 23

Regulator napięcia

Za kontrolę generowanego napięcia odpowiedzialny jest cyfrowy regulator napięcia. Stabilność napięcia wynosi ±1% w stanie ustalonym niezależnie od współczynnika mocy oraz zmiany obrotów w zakresie od -5% do +30% obrotów znamionowych.

Uzwojenia / System wzbudzenia

Stojan alternatora jest nawinięty z poskokiem 2/3. Zapewnia to eliminację krotności trzeciej harmonicznej (3, 9, 15, itd.) napięcia wyjściowego. Uznawane jest to za najlepsze rozwiązanie w celu niezawodnego zasilania odbiorników nieliniowych. Poskok 2/3 minimalizuje indukowanie się nadmiernych prądów w obwodzie neutralnym. Uzwojenie Dodatkowe jest oddzielnym uzwojeniem w stojanie zasilającym regulator napięcia. **Uzwojenie to umożliwia przejęcie 300% obciążenia znamionowego przez 20 sekund**. Umożliwia to niezawodny rozruch silników elektrycznych. Izolacja / Impregnacja Izolacja jest klasy H. Uzwojenia zostały zaimpregnowane najwyższej jakości żywicą epoksydową Normy wykonania Alternator został wykonany zgodnie z najbardziej powszechnymi normami, tj. CEI 2-3, IEC 34-1, EN

Wyposażenie agregatu :

PODSTAWA WYKONANA ZE SPAWANYCH STALOWYCH PROFILI, WYPOSAŻONA W:

• Amortyzatory drgań o odpowiedniej wielkości

- Spawane nogi podporowe

PLASTIKOWY ZBIORNIK PALIWA WYPOSAŻONY W:

- Wlew
- Odmę (wentylację)
- Czujnik poziomu paliwa
- Pojemność zbiornika paliwa - 80 L
- Czas pracy przy @ 75% PRP h – min 10 h

RURKA SPUSTOWA OLEJU:

- Ułatwiony spust oleju

OPCJE PANELU STEROWANIA:

- Wiele języków wyświetlania
- Pięć klawiszy nawigacyjnych menu
- Wskaźnik alarmu LCD
- Dostępna opcja podgrzewanego wyświetlacza
- Możliwość dostosowania tekstu i obrazów do zasilania
- Możliwość rejestrowania danych
- Wewnętrzny edytor PLC
- Funkcja wyłączania zabezpieczeń
- W pełni konfigurowalny za pomocą komputera PC USB, RS232 i RS485 komunikacja
- Tryb oszczędzania energii
- Monitorowanie prądu i mocy generatora (kW, kvar, kVA, pf)
- Prąd sieciowy i moc monitorowanie (kW, kvar, kVA, pf
- Alarmy przeciążenia kW
- Zabezpieczenie przed nierównomiernym obciążeniem
- Niezależna ochrona przed zwarciem doziemnym
- Sterowanie wyłącznikiem za pomocą przycisków na panelu przednim
- 6 konfigurowalnych wyjść DC
- 2 konfigurowalne wyjścia przekaźnikowe beznapięciowe
- 6 konfigurowalnych wejść analogowych/ cyfrowych
- Obsługa czujników 0 V do 10 V i 4 mA do 20 mA
- 8 konfigurowalnych wejść cyfrowych
- Zegar czasu rzeczywistego
- Jednoczesne korzystanie z portów komunikacyjnych RS232 i RS485
- Obsługa protokołu MODBUS RTU
- Wysyłanie wiadomości SMS (wymagany dodatkowy modem zewnętrzny)

STEROWANIE I INNE

- Tryby pracy: OFF - Ręczny start - Automatyczny start - Automatyczny test
- Przyciski wymuszenia zasilania z agregatu lub z sieci

- Przyciski: start/stop, reset błędu, góra/dół/strona/wybór
- Wyłącznik awaryjny agregatu
- Możliwość zdalnego startu.
- Alarm dźwiękowy
- Port komunikacyjny wbudowany w panel sterowania agregatem
- Wyłącznik zasilania DC
- Automatyczny prostownik akumulatora

ZABEZPIECZENIA Z ALARMEM

- Zabezpieczenia silnika: niski poziom paliwa, niskie ciśnienie oleju, wysoka temperatura sinika
- Zabezpieczenia agregatu: niskie/wysokie napięcie, przeciążenie, niska/wysoka częstotliwość, nieudany rozruch, niskie/wysokie napięcie akumulatora, awaria prostownika akumulatora

ZABEZPIECZENIA Z WYŁĄCZENIEM

- Zabezpieczenia silnika: niski poziom paliwa, niskie ciśnienie oleju, wysoka temperatura sinika

INNE ZABEZPIECZENIA

- Wyłącznik awaryjny.
- Panel zabezpieczony zamykanymi drzwiami

MONTAŻ AGREGATU:

Zamawiający wymaga aby wykonawca dostarczył, rozładował a także zamontował agregat prądotwórczy.
Za montaż uważa się wykonanie wszelkich niezbędnych prac w tym także budowa podestu/kostki pod agregat, przebić, kopania, montażu układu/układów SZR I podłączenie do agregatu prądotwórczego oraz wykonanie prób poprawnego działania całego systemu.

AUTOMATYKA SZR/ATS:

Zamawiający aby wykonawca dostarczył układy SZR /ATS- automatykę serującą- przełączaniem zasilania obwodów dopasowaną do agregatu I stanu istniejącego instalacji elektrycznej.
Przełącznik SZR/ATS z możliwością przełączania ręcznego oraz automatycznego uniemożliwiający przedostanie się napięcia z agregatu na siec i odwrotnie.

W celu doboru rozwiązania wykonawca wymaga dokonania wizji lokalnej.

VI Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV)

CPV 48820000-2
CPV 72268000-1
CPV 72263000-6
CPV 79212000-3
CPV 80550000-4
CPV 31122000-7

VII Miejsce i Terminy wykonania zamówienia

Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Część 1, 2 i 5 będzie realizowana w ciągu 21 dni, część 3 w ciągu 120 dni, część 4 w ciągu 180 dni, liczonego od dnia podpisania umowy w przedmiocie udzielenie zamówienia publicznego.

Przedmiot umowy będzie dostarczany przez Wykonawcę do miejsc wskazanych przez Zamawiającego w zakresie dostawy sprzętu/oprogramowania/licencji.

Zamawiający może zawrzeć umowę w sprawie przedmiotowego zamówienia publicznego przed upływem terminu, jeżeli w przedmiotowym postępowaniu zostanie złożona tylko jedna oferta.

VIII Warunki udziału w postępowaniu

1. udzielenie zamówienia mogą się ubiegać wykonawcy, którzy:
    - nie podlegają wykluczeniu na podstawie ustawy prawo zamówień publicznych,
    - spełniają warunki udziału w postępowaniu w zakresie kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile obowiązek ich posiadania wynika z odrębnych przepisów. Zamawiający nie określa szczegółowo ww. warunku.
    - spełniają warunki udziału w postępowaniu w zakresie sytuacji ekonomicznej lub finansowej. Zamawiający nie określa szczegółowo ww. warunku.
    - spełniają warunki udziału w postępowaniu w zakresie zdolności technicznej lub zawodowej.
2. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Na potwierdzenie spełnienia warunku udziału w postępowaniu, dotyczącego zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca wykazał się odpowiednim doświadczeniem, do części 1 Zamówienia, tj. w ciągu ostatnich 3 lat przed upływem terminu składania ofert, w tym okresie realizuje, bądź zrealizował należycie co najmniej dwie usługi w zakresie dostawy sprzętu komputerowego na kwotę co najmniej 200 000 złotych.
4. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
5. Wykonawca, który polega na zdolnościach innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych

podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

IX Przesłanki wykluczenia Wykonawcy

1. Zamawiający wykluczy wykonawcę z postępowania o udzielenie zamówienia, w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych w art. 108 ust. 1 ustawy Pzp, tj.:

   1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
   a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
   b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
   c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz.U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust.1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz.U. z 2021 r. poz. 523, 1292, 1559 i 2054),
   d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
   e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
   f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),
   g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
   h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej - lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego; 2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
   3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
2. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
3. jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16

lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie.

4. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.
5. Zamawiający nie wprowadza w tym postępowaniu dodatkowych podstaw wykluczenia wskazanych w art. 109 ustawy Pzp.
6. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy Pzp.
7. Jeżeli wykonawca polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby zamawiający zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.
8. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia zgodnie z art. 110 ust. 1 ustawy Pzp.
9. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt. 1, 2 i 5 ustawy Pzp, jeśli udowodni zamawiającemu, że spełnił przesłanki wskazane w art. 110 ust. 2 ustawy Pzp. Zamawiający oceni, czy podjęte przez wykonawcę czynności o których mowa w art. 110 ust. 2 ustawy Pzp są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności, o których mowa w art. 110 ust. 2 ustawy Pzp, nie są wystarczające do wykazania rzetelności, zamawiający wykluczy wykonawcę.
10. Ponadto Zamawiający wykluczy z postępowania o udzielenie zamówienia Wykonawcę, w stosunku, do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 7 ust. 1 zgodnie z ustawą o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z dnia 13 kwietnia 2022 roku (Dz. U. z 2022, poz. 835).

X Obowiązek zatrudniania przez wykonawcę osób na podstawie stosunku pracy (art. 95 PZP)

1. Zamawiający wymaga aby osoby wskazane w wykazie osób odpowiedzialne za wykonanie zamówienia po Stronie Wykonawcy zatrudnione były na podstawie stosunku pracy, o którym mowa w art. 22 § 1 Kodeksu pracy.

2. Wykonawca zobowiązuje się, że pracownicy wykonujący czynności wchodzące w skład tzw. kosztów bezpośrednich, wykonywane przez pracowników (wskazanych powyżej) będą w okresie realizacji przedmiotu zamówienia zatrudnieni na podstawie umowy o pracę w rozumieniu przepisów ustawy z dnia 26 czerwca 1974r. – Kodeks pracy (jeżeli ten obowiązek wynika z art. 22 §1 Kodeksu pracy).
3. Obowiązek określony powyżej dotyczy również podwykonawców
4. W celu weryfikacji zatrudniania, przez wykonawcę lub podwykonawcę, na podstawie umowy o pracę, osób wykonujących wskazane przez zamawiającego czynności w zakresie realizacji zamówienia, Zamawiający wymaga złożenia oświadczenia wykonawcy lub podwykonawcy o zatrudnieniu pracownika na podstawie umowy o pracę.
5. Pozostałe osoby uczestniczące w wykonaniu zamówienia mogą współpracować z Wykonawcą na podstawie umów cywilnoprawnych.
6. W przypadku uzasadnionych wątpliwości co do przestrzegania prawa pracy przez Wykonawcę lub Podwykonawcę, Zamawiający może zwrócić się o przeprowadzenie kontroli przez Państwową Inspekcję Pracy.

XI Wykaz oświadczeń lub dokumentów, jakie mają złożyć wykonawcy w celu wykazania spełniania warunków udziału w postępowaniu oraz niepodlegania wykluczeniu z postępowania

1. Wykaz podmiotowych środków dowodowych: 3.1. Zgodnie z art. 274 ust. 1 ustawy Pzp, zamawiający przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia, następujących podmiotowych środków dowodowych:

- Wykaz dostaw wykonanych w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - tj.w tym okresie, wraz z podaniem ich wartości, dat wykonania i podmiotów na rzecz, których usługi zostały wykonane, przed upływem terminu składania ofert, w co najmniej dwóch usług w zakresie dostawy sprzętu komputerowego na kwotę co najmniej 500 000 złotych wraz z dowodem należytego ich wykonania.
- Aktualne na dzień składania ofert oświadczenia, stanowiące wstępne potwierdzenie, że nie podlega wykluczeniu z postępowania,
- Aktualne na dzień składania ofert oświadczenie sankcyjne,
- Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu, zamieszcza informacje o tych podmiotach w oświadczeniach,

2 Zamawiający wymaga od Wykonawcy złożenia wraz z ofertą następujących przedmiotowych środków dowodowych w celu potwierdzenia zgodności oferowanych produktów z wymaganiami Zamawiającego w zakresie wskazanym w zestawieniu poniżej:

- do części 3 Zamówienia; co najmniej dwa z trzech certyfikatów: MS 50255 Managing, Maintaining, and Securing Your Networks Through Group Policy, SC-900 Microsoft Certified: Security, Compliance, and Identity Fundamentals, MS-55341 Installation, Storage, and Compute with Windows Server, w zakresie usług i rozwiązań opartych o środowisko Microsoft;
- do części 4 Zamówienia; ITIL® Foundation Certificate in IT Service Management w zakresie projektowania, zrozumienia i zastosowania najlepszych praktyk w zarządzaniu usługami informatycznymi;
- do części 4 Zamówienia; co najmniej dwa z trzech certyfikatów: Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE), Certified Professional Penetration Tester (eCPPTv2) w zakresie testowania I weryfikacji poprawności wdrażanych rozwiązań,

3. W odniesieniu do pozostałych przedmiotowych środków dowodowych zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane dostawy spełniają określone przez zamawiającego wymagania, cechy i kryteria.
4. Zamawiający informuje, że działając na podstawie art. 107 ust. 2 ustawy Pzp przewiduje, że w sytuacji, w której Wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, Zamawiający jednokrotnie wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.

Postanowień pkt 4 SWZ nie stosuje się:

a) w części w jakiej przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub,

b) pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.

Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści przedmiotowych środków dowodowych.

5. Wykonawca jest zobowiązany do wypełnienia obowiązku informacyjnego przewidzianego w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał (w przypadku korzystania z podwykonawców/ podmiotów trzecich/wykonawców wchodzących w skład konsorcjum) w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

XII Podwykonawcy

1. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z wnioskiem o dopuszczenie do udziału w postępowaniu albo odpowiednio wraz z ofertą, zobowiązanie podmiotu trzeciego do oddania do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.

2. Zobowiązanie podmiotu udostępniającego zasoby potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   - zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
   - sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   - czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje dostawy lub usługi, których wskazane zdolności dotyczą.
3. Podwykonawcy obowiązani są do złożenia wszelkich oświadczeń, w szczególności oświadczeń sankcyjnych i o braku przesłanek wykluczenia w takim zakresie w jakim dotyczą one Wykonawcy.

XIII Informacja dla wykonawców polegających na zasobach innych podmiotów, na zasadach określonych w art. 118 ustawy PZP

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
4. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
5. Zobowiązanie podmiotu udostępniającego zasoby lub inny środek dowodowy, o którym mowa w pkt 9.4 SWZ potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
6. 1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;

7.2) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;

8.3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.

9. Zamawiający oceni, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu a także zbada, czy nie zachodzą, wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
10. Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą, wobec tego podmiotu podstawy wykluczenia, Zamawiający zażąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
11. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia oświadczenia podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.

XIV Kryterium równoważności

1. Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych rozwiązaniom wskazanym przez Zamawiającego. Wykonawca oferując rozwiązanie równoważne do opisanego powyżej jest zobowiązany wykazać (udowodnić) równoważność w zakresie wskazanych parametrów, które muszą być na poziomie nie gorszym niż parametry wskazane przez Zamawiającego - Wykonawca musi wykazać (udowodnić), iż proponowane rozwiązanie w równoważnym stopniu spełnia wymagania określone w zapytaniu ofertowym, w szczególności w zakresie parametrów. Jeżeli w opisie przedmiotu zamówienia znajdują się jakiekolwiek odniesienia do określonego wyrobu, źródła, znaków towarowych, patentów czy pochodzenia lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę – należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza składanie ofert równoważnych, w szczególności o parametrach technicznych, użytkowych, funkcjonalnych i jakościowych nie gorszych niż te, podane w opisie przedmiotu zamówienia.

XV Opis sposobu składania ofert w postępowaniu

1. Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej.
2. Preferuje się , aby komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane były za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do zamawiającego".Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego" po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego. Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
3. Ofertę wraz z oświadczeniami i dokumentami należy złożyć w terminie do dnia 17 kwietnia 2025 roku do godziny 10;00 za pośrednictwem platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/um_pyrzyce
4. Oferta powinna zawierać:

   Formularz oferty;

   - Pełnomocnictwo do reprezentowania Wykonawcy, w tym podpisania oferty, o ile prawo do podpisania oferty nie wynika z innych dokumentów złożonych wraz z ofertą. Treść pełnomocnictwa musi jednoznacznie określać czynności, co do wykonywania których pełnomocnik jest upoważniony;
   - Wyjaśnienia uzasadniające zastrzeżenie tajemnicy przedsiębiorstwa (jeżeli dotyczy);
   - Oświadczenia i dokumenty o których mowa w treści niniejszej SWZ.
5. Otwarcie ofert nastąpi w dniu 17 kwietnia 2025 roku o godz. 10;30.
6. Wykonawca nie może wprowadzić zmian do złożonej oferty.
7. Wykonawca może przed upływem terminu składania ofert wycofać ofertę.

XVI Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	90
2.	Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę	10

2. Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.
3. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.
4. Przy ocenie ofert w kryterium „Cena" (C) punkty zostaną przyznane w poniższy sposób:
   - Cena – znaczenie 90% (maksymalnie do 90 pkt)
   - Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
   - Punkty w kryterium „Cena" będą obliczane na podstawie wzoru:

C = CC min/ CC of x 90

gdzie:

C – punkty przyznane Wykonawcy w ramach kryterium „Cena"

CC min – najniższa cena brutto spośród badanych ofert

CC of – cena brutto badanej ofert

   - Do wzoru zostaną przyjęte ceny podane przez Wykonawców w Formularzu Oferty stanowiącym Załącznik nr 1 do SWZ.

5. Kryterium „Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę" stanowi 10 możliwych do uzyskania punktów.

6. Sumaryczna liczba punktów zostanie obliczona według wzoru:

   W = C + E

   gdzie:

   W – łączna liczba punktów przyznanych w poszczególnych kryteriach,

   C – liczba punktów przyznanych w kryterium „Cena",

   E – wartość punktowa kryterium „Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę",

Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku

7. Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.

8. W związku z zaistnieniem przesłanki o której mowa w art. 246 ust. 2 PZP możliwe było zastosowanie kryterium ceny jako kryterium o wadze przekraczającej 60%, ze względu na określenie w opisie przedmiotu zamówienia wymagań jakościowych odnoszących się do co najmniej głównych elementów składających się na przedmiot zamówienia.

XVII Wzór umowy

1. Załącznik nr 2 Istotne Postanowienia Umowy Część 1
2. Załącznik nr 3 Istotne Postanowienia Umowy Część 2
3. Załącznik nr 4 Istotne Postanowienia Umowy Część 3
4. Załącznik nr 5 Istotne Postanowienia Umowy Część 4
5. Załącznik nr 6 Istotne Postanowienia Umowy Część 5

XVIII RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z dnia 4 maja 2016 r., str. 1), dalej „RODO", informuję, że:

1) administratorem Pani/Pana danych osobowych jest Burmistrz Pyrzyc, Plac Ratuszowy 1, 74-200 Pyrzyce;

2) Inspektor ochrony danych urzęduje w Urzędzie Miejskim w Pyrzycach , Plac Ratuszowy 1, 74-200 Pyrzyce, tel. 91 39 70 317, e-mail: iod@pyrzyce.um.gov.pl w godzinach w poniedziałki 800-1600, w pozostałe dni tygodnia w godzinach 700-1500;

3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn **„Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd" w Gminie Pyrzyce w ramach: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (DERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd"**

4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 Ustawy,

5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 Ustawy, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach Ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z Ustawy;

7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;

8) posiada Pani/Pan:

a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;

c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;

d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9) nie przysługuje Pani/Panu:

a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

XIX Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej

1. Zamawiający pracuje w następujących dniach i godzinach: w poniedziałek 8:00 – 16:00; od wtorku do piątku w godz: 7:00 – 15:00

2. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym, a Wykonawcami odbywa się wyłącznie przy użyciu strony internetowej https://platformazakupowa.pl/pn/um_pyrzyce

3. Link do postępowania dostępny jest na Profilu Nabywcy Zamawiającego:

1) Osobami uprawnionymi do bezpośredniego kontaktowania się z wykonawcami są:

• Koordynator Projektu - od godz. 8.00 do 15.00 – Kazimierz Jaborowski tel. 91 39 70 322, e-mail: obrona_cywilna@pyrzyce.um.gov.pl

• w zakresie przedmiotu zamówienia - od godz. 8.00 do 15.00 – Damian Kogut tel. 91 39 70 317 , e-mail: informatyk@pyrzyce.um.gov.pl

• w zakresie przedmiotu zamówienia - od godz. 8.00 do 15.00 – Artur Zibrowski tel. 91 39 70 372 , e-mail: nfo@pyrzyce.um.gov.pl

• w zakresie dotyczącym zgodności z procedurami - od godz. 8.00 do 15.00 – Sylwia Ranoszek tel. 91 39 70 346 , e-mail: s.ranoszek@pyrzyce.um.gov.pl

2) Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w regulaminie.

3) Instrukcja składania ofert oraz sposobu komunikowania się Zamawiającego z Wykonawcami, zwana dalej „instrukcją", jest integralną częścią platformazakupowa.pl i dostępna jest na stronie dotyczącej prowadzonego postępowania.

4) W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami, w szczególności składanie oświadczeń, zawiadomień oraz przekazywanie informacji (np. zadawanie pytań, uzupełnianie oświadczeń lub dokumentów na wezwanie Zamawiającego) odbywa się elektronicznie za pośrednictwem strony internetowej formularza Wyślij wiadomość dostępnego na stronie dotyczącej prowadzonego postępowania.

5) Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych (Dz. U. z 2017 r. poz. 1320 ze zm.) oraz rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz.U. 2020r. poz. 2415).

6) Zgodnie z art. 8 ustawy Pzp, :

- termin oznaczony w godzinach rozpoczyna się z początkiem pierwszej godziny i kończy się z upływem ostatniej godziny.

- jeżeli początkiem terminu oznaczonego w godzinach jest pewne zdarzenie, nie uwzględnia się przy obliczaniu terminu godziny, w której to zdarzenie nastąpiło.

- termin obejmujący dwa lub więcej dni zawiera co najmniej dwa dni robocze.

- dniem roboczym nie jest dzień uznany ustawowo za wolny od pracy oraz sobota.

7) Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści specyfikacji. Zamawiający jest zobowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed terminem składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści specyfikacji wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.

8) W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa Części VIII. pkt.8.3.7), Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużania terminu składania ofert.

9) Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o wyjaśnienie treści SWZ.

10) Treść zapytań wraz z wyjaśnieniami Zamawiający udostępnia, bez ujawniania źródła zapytania na stronie prowadzonego postępowania, na której udostępnił specyfikację.

11) Wszelkie pytania i wątpliwości dotyczące prowadzonego postępowania należy kierować przy użyciu https://platformazakupowa.pl/pn/um_pyrzyce

12) Wszelkie modyfikacje, uzupełnienia i ustalenia oraz zmiany, w tym zmiany terminów, jak również pytania wykonawców wraz z wyjaśnieniami stają się integralną częścią specyfikacji i będą wiążące przy składaniu ofert.

4. Zamawiający nie zamierza zwoływać zebrania Wykonawców w celu wyjaśnienia treści SWZ.

5. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść specyfikacji istotnych warunków zamówienia. Dokonaną w ten sposób modyfikację udostępnia za pośrednictwem https://platformazakupowa.pl/pn/um_pyrzyce

6. Zamawiający przedłuży termin składania ofert, jeżeli w wyniku zmiany treści specyfikacji warunków zamówienia niezbędny jest dodatkowy czas na wprowadzenie zmian w ofertach. O przedłużeniu terminu składania ofert Zamawiający niezwłocznie zawiadamia za pośrednictwem https://platformazakupowa.pl/pn/um_pyrzyce

W przypadku rozbieżności pomiędzy treścią specyfikacji warunków zamówienia, a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.

Specyfikacja połączenia, formatu przesyłanych danych oraz kodowania i oznaczania czasu odbioru danych Systemu e-ZP:

a) Format kodowania treści w obrębie Systemu - UTF8,

b) Komunikacja pomiędzy przeglądarką Wykonawcy, a serwerem jest wykonywana przy użyciu bezpiecznego protokołu HTTPS,

c) Oznaczeniem czasu odbioru danych przez System jest data oraz dokładny czas (hh: mm: ss) - czas lokalny serwera synchronizowany odpowiednim źródłem czasu.

Wymagania techniczne związane z korzystaniem z Systemu (tj. informacje dotyczące specyfikacji połączenia, formatu przesyłanych danych oraz kodowania i oznaczania czasu przekazania danych):

a) stały dostęp do sieci Internet i minimalna prędkość połączenia internetowego nie mniejsza niż 512 kb/s;

b) zaktualizowana przeglądarka internetowa Chrome w wersji 77 i późniejsze lub Mozilla Firefox w wersji 63 i późniejsze;

c) system operacyjny Microsoft Windows 7 i późniejsze lub Apple macOS 10.14 i późniejsze, dystrybucje systemu Linux;

d) korzystanie z wbudowanej w System e-ZP funkcjonalności składania podpisu elektronicznego możliwe jest pod warunkiem, że system teleinformatyczny, z którego korzysta Wykonawca, wyposażony jest w jeden z poniższych komponentów:

- wirtualna maszyna Java firmy Oracle w wersji co najmniej 1.8.0_221 (Java SE JRE 8 Update 221) z obsługą technologii Java Web Start (JavaWS) lub

- wirtualna maszyna OpenJDK w wersji co najmniej 1.8.0_222 z zainstalowanym rozszerzeniem IcedTea Web Start.

Powyższe wymagania nie ograniczają możliwości korzystania przez Wykonawcę z zewnętrznego oprogramowania do składania podpisu elektronicznego:

a) kwalifikowany podpis elektroniczny (dopuszczalne formaty podpisów: PaDES - format.pdf, XaDES - pozostałe formaty);

b) podpis zaufany;

c) certyfikat osobisty;

d) dopuszczalne formaty danych: .txt, .pdf, .xls, .doc,.docx, .rtf, .odt, .rtf, .xml (zalecany .pdf);

e) maksymalny rozmiar przesyłanych plików złożenia, wycofania oferty oraz wiadomości wynosi 150 MB;

f) w zakresie dotyczącym kodowania i czasu odbioru danych Zamawiający informuje, że złożona przez Wykonawcę za pomocą Systemu e-ZP oferta jest widoczna w systemie, jako zaszyfrowana, a możliwość jej odszyfrowania i otworzenia przez Zamawiającego możliwa jest po upływie terminu składania ofert.

W zależności od formatu podpisu: Podpis kwalifikowany (PAdES, XAdES), podpis osobisty (XAdES), podpis zaufany (PAdES, XAdES) i jego typu (zewnętrzny, otaczający) Wykonawca dołącza do Systemu e-ZP uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z podpisem (typ otaczający).

Sposób sporządzenia dokumentów elektronicznych musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 poz. 2452) oraz rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. z 2020 poz. 2415) oraz rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (załącznik nr 2 do Rozporządzenia).

Wykonawca może zwrócić się do Zamawiającego o wyjaśnienia dotyczące wszelkich wątpliwości związanych z SWZ, przedmiotem zamówienia, sposobem przygotowania i złożenia oferty.

Zamawiający udzieli wyjaśnień zgodnie z art. 284 ustawy Pzp.

Zamawiający umieści wyjaśnienia w Systemie e-ZP bez ujawnienia źródeł zapytania. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ.

Ofertę składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa następnie wraz z plikami stanowiącymi jawną część należy ten plik zaszyfrować.

Do oferty należy dołączyć oświadczenie o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, a następnie zaszyfrować wraz z plikami stanowiącymi ofertę.

Oferta może być złożona tylko do upływu terminu składania ofert.
Wykonawca może przed upływem terminu do składania ofert wycofać ofertę.
Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

XX Sposób obliczenia ceny

1. Wykonawca poda cenę oferty w Formularzu Ofertowym jako cenę brutto [z uwzględnieniem kwoty podatku od towarów i usług (VAT)] z wyszczególnieniem stawki podatku od towarów i usług (VAT).
2. Cena oferty stanowi wynagrodzenie ryczałtowe.
3. Cena musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
4. Wykonawca poda w Formularzu Ofertowym stawkę podatku od towarów i usług (VAT) właściwą dla przedmiotu zamówienia, obowiązującą według stanu prawnego na dzień składania ofert. Określenie ceny ofertowej z zastosowaniem nieprawidłowej stawki podatku od towarów i usług (VAT) potraktowane będzie, jako błąd w obliczeniu ceny i spowoduje odrzucenie oferty,
5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).

6. W przypadku rozbieżności pomiędzy ceną ryczałtową podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena ryczałtowa podana słownie.

XXI Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający zawiera umową w sprawie zamówienia publicznego, z uwzględnieniem art. 577 pzp, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umową w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertą.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o miejscu i terminie podpisania umowy.
4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią Załącznik Nr 2 do SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.
5. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty jako najkorzystniejszej) przedstawią Zamawiającemu umowę regulującą współpracę tych Wykonawców.
6. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

XXII Środki ochrony prawnej

1. Środki ochrony prawnej przewidziane są w dziale IX ustawy.

2. Środkami ochrony prawnej są odwołanie i skarga do sądu.

3. Środki ochrony prawnej przysługują wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz

dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 ustawy Pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.

4 Odwołanie przysługuje na:

1) niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;

2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy;

3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.

23.5 Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, że zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.

6 Terminy wnoszenia odwołań.

1) Odwołanie wnosi się w terminie:

a) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,

b) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a.

7. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej.

8. Odwołanie w przypadkach innych niż określone w pkt 1 i 2 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest mniejsza niż progi unijne.

9. Jeżeli zamawiający nie opublikował ogłoszenia o zamiarze zawarcia umowy lub mimo takiego obowiązku nie przesłał wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty lub nie zaprosił wykonawcy do złożenia oferty w ramach dynamicznego systemu zakupów lub umowy ramowej, odwołanie wnosi się nie później niż w terminie:

1) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania

2) miesiąca od dnia zawarcia umowy, jeżeli zamawiający:

a) nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo

b) zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o wyniku postępowania, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki.

10. Odwołanie zawiera:

1) imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres

poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);

2) nazwę i siedzibę zamawiającego, numer telefonu oraz adres poczty elektronicznej zamawiającego;

3) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub NIP odwołującego będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania albo posiada go nie mając takiego obowiązku;

4) numer w Krajowym Rejestrze Sądowym, a w przypadku jego braku - numer w innym właściwym rejestrze, ewidencji lub NIP odwołującego niebędącego osobą fizyczną, który nie ma obowiązku wpisu we właściwym rejestrze lub ewidencji, jeżeli jest on obowiązany do jego posiadania;

5) określenie przedmiotu zamówienia;

6) wskazanie numeru ogłoszenia w przypadku zamieszczenia w Biuletynie Zamówień Publicznych albo publikacji w Dzienniku Urzędowym Unii Europejskiej;

7) wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, lub wskazanie zaniechania przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy;

8) zwięzłe przedstawienie zarzutów;

9) żądanie co do sposobu rozstrzygnięcia odwołania;

10) wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności;

11) podpis odwołującego albo jego przedstawiciela lub przedstawicieli;

12) wykaz załączników.

Do odwołania dołącza się:

1) dowód uiszczenia wpisu od odwołania w wymaganej wysokości;

2) dowód przekazania odpowiednio odwołania albo jego kopii zamawiającemu;

3) dokument potwierdzający umocowanie do reprezentowania odwołującego.

11. Na orzeczenie Izby stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych.

ZAŁĄCZNIKI

Załącznik nr 1 Formularz oferty
Załącznik nr 2 Istotne Postanowienia Umowy Część 1
Załącznik nr 3 Istotne Postanowienia Umowy Część 2
Załącznik nr 4 Istotne Postanowienia Umowy Część 3
Załącznik nr 5 Istotne Postanowienia Umowy Część 4
Załącznik nr 6 Istotne Postanowienia Umowy Część 5
Załącznik nr 7 Oświadczenie wykonawcy
Załącznik nr 8 RODO Pozyskiwanie ofert na usługi dostawy roboty - wykonawcy
Załącznik nr 9 RODO Pozyskiwanie ofert na usługi dostawy roboty - reprezentanci wykonawcy
Załącznik nr 10 Oświadczenie o spełnieniu warunków udziału w postępowaniu

Z-CA BURMISTRZA
Karolina Radziewicz

p.o. Z-CY KIEROWNIKA
Beata Wiwała

MŁ. REFERENT ds. OCIZK
Kazimierz Jaborowski

INFORMATYK
Damian Kogut