



SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego pn.:

Dostawa sprzętu i oprogramowania w ramach projektu

„Cyberbezpieczny samorząd” w Gminie Sępólno

w ramach: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II:

Zaawansowane usługi cyfrowe Działanie 2.2 – Wzmocnienie krajowego systemu

cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego

„Cyberbezpieczny Samorząd”

Znak sprawy: Or.III.271.1.9.2025

Spis treści

I ZAMAWIAJĄCY	4
II Definicje	5
III Wartość zamówienia.....	6
IV Opis przedmiotu zamówienia	6
V Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV).....	69
VI Miejsce i Terminy wykonania zamówienia	70
VII Warunki udziału w postępowaniu	70
VIII Przesłanki wykluczenia Wykonawcy	70
IX Obowiązek zatrudniania przez wykonawcę osób na podstawie stosunku pracy (art. 95 PZP)	72
X Wykaz oświadczeń lub dokumentów, jakie mają złożyć wykonawcy w celu wykazania spełniania warunków udziału w postępowaniu oraz niepodlegania wykluczeniu z postępowania	72
XI Poleganie na zasobach podmiotów trzecich.....	73
XII Podwykonawstwo	74
XIII Informacja dla wykonawców polegających na zasobach innych podmiotów, na zasadach określonych w art. 118 ustawy PZP	74
XIV Kryterium równoważności	75
XV Opis sposobu składania ofert w postępowaniu	75
XVI Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem wag tych kryteriów i sposobu oceny ofert.....	76

XVII Wzór umowy.....	78
XVIII RODO	78
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.....	79
XX Sposób obliczenia ceny	81
XXI Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego	81
XXII Środki ochrony prawnej.....	82
XXIII ZAŁĄCZNIKI.....	83

I ZAMAWIAJĄCY **Gmina Sępól****GMINA SĘPOPOL****ul. 11 Listopada 7, 11-210 Sępól****Tel. 89 761 31 81****<https://bipsepopol.pl>****NIP : 743 20 21 679 REGON: 510743628****Godziny pracy : poniedziałek 8:00 – 16:00****wtorek-piątek 7:15 – 15:15**

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. (z.u. z 2024 r. poz. 1320) 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 **24.07.2025 r.** W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa w 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, obowiązującą 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. (tj .Dz.U. z 2024 r. poz. 1320 ze zm.).

IV Opis przedmiotu zamówienia

CZĘŚĆ I

1. Serwer I – 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	- Obudowa Rack o wysokości max 1U 8 wnęk na dyski 2.5" Hot-Plug - Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej - 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. - Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci - Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor 8-rdzeniowy, min. 2.8GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 127 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	32GB DDR4 RDIMM 3200MT/s,
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
Dyski twarde	- Zainstalowane: 2x dysk SAS o pojemności min. 1.2TB, Hot-Plug. - Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Gniazda PCI	Jeden slot PCIe LP
Interfejsy sieciowe/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet BaseT

Wbudowane porty	• Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, • Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0, • 1x LAN 2,5Gb/s
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	• Redundantne
Zasilacze	• Redundantne, Hot-Plug maksymalnie 700W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	• Windows Server 2025 Essentials
Bezpieczeństwo	• Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane SSL ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ integracja z Active Directory; ○ wsparcie dla automatycznej rejestracji DNS

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

- 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.

Oprogramowanie do monitorowania

Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:

- Monitoring:

- ilość podłączonych oraz rozłączonych systemów
- stan podłączonych urządzeń
- informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
- Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
- informacje o statusie gwarancji dla poszczególnych urządzeń
- informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
- informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
- Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych
- Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.

- Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
- Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
- Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
- Monitoring parametrów serwerów z informacją o minimum:
 - Obciążeniu procesora
 - Zużyciu pamięci RAM
 - Temperaturze procesorów
 - Temperaturze powietrza wlotowego
 - Zużyciu prądu
 - Zmianach w fizycznej konfiguracji serwera
 - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Monitoring parametrów pamięci masowych z informacją o minimum:
 - Opóźnieniach
 - IOPS
 - Przepustowości
 - Utylizacji kontrolerów
 - Pojemność całkowita i dostępna
 - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
 - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
 - Informacje o poziomie redukcji danych
 - Informacje o statusie replikacji oraz snapshotów
- Monitoring parametrów przełączników sieciowych z informacją o minimum:
 - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
 - Stanie komponentów: zasilacze, wentylatory
 - Podłączonych hostach
 - Ilości i statusu portów
 - Utylizacji procesora
 - Utylizacji poszczególnych portów
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Aktualizacja firmware
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania

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

Certyfikaty

- 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 Bronze 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 3 lat. - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. - Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. - Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/porta) 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. - 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 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 wsparciem 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 prześle 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 autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

2. Serwer II – 1 sztuka

Obudowa	• Obudowa typu Tower z możliwością instalacji 3 dysków twardych 3.5".
Płyta główna	• Płyta główna z możliwością instalacji jednego fizycznego procesora, • Płyta główna posiadająca minimum 4 sloty na pamięć RAM UDIMM z możliwością zainstalowania do minimum 128GB pamięci RAM, • Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	• Zainstalowany jeden procesor min. 4-rdzeniowy, min. 2.6GHz, klasy x86, dedykowany do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min. 39.6 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org.
Pamięć RAM	• 2x16 GB pamięci RAM UDIMM o częstotliwości taktowania minimum 5600MHz
Kontroler RAID	• Możliwość konfiguracji poziomów RAID: 0, 1, 5, 10
Dyski twarde	• Zainstalowane: ○ 2 dysk SSD SATA o pojemności min. 960GB • Możliwość instalacji dwóch dysków M.2 NVMe SSD o pojemności min. 480GB oraz możliwość konfiguracji w RAID1.
Sloty PCI Express	• Dwa sloty PCI Express
Interfejsy sieciowe/FC/SAS	• Minimum dwa interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCI Express.

Wbudowane porty	• Minimum 8 portów USB z czego min. 5 w technologii 3.0 • 1x RS-232 • 1x VGA • 1x LAN 2,5Gb/s
Video	• Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Zasilacz	• Maksymalnie 500W
System operacyjny/dodatki e oprogramowanie	• Windows Server 2025 Essentials • Nośnik CD/DVD z plikiem instalacyjnym Windows Server 2022 Essentials
Bezpieczeństwo	• 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 w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • 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 autentykację 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.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewni proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: - Monitoring: - ilość podłączonych oraz rozłączonych systemów - stan podłączonych urządzeń - informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów - Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia - informacje o statusie gwarancji dla poszczególnych urządzeń - informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń - informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. - Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych - Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. - Monitorowanie wydajności, przepustowości oraz opóźnień dla systemu pamięci masowych. - Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. - Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. - Monitoring parametrów serwerów z informacją o minimum: - Obciążeniu procesora - Zużyciu pamięci RAM - Temperaturze procesorów - Temperaturze powietrza wlotowego - Zużyciu prądu - Zmianach w fizycznej konfiguracji serwera

- Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Monitoring parametrów pamięci masowych z informacją o minimum:
 - Opóźnieniach
 - IOPS
 - Przepustowości
 - Utylizacji kontrolerów
 - Pojemność całkowita i dostępna
 - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
 - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
 - Informacje o poziomie redukcji danych
 - Informacje o statusie replikacji oraz snapshotów
- Monitoring parametrów przełączników sieciowych z informacją o minimum:
 - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
 - Stanie komponentów: zasilacze, wentylatory
 - Podłączonych hostach
 - Ilości i statusu portów
 - Utylizacji procesora
 - Utylizacji poszczególnych portów
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Aktualizacja firmware
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
 - Możliwość generowania raportów dla serwerów zawierających informację o:
 - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
 - Średnim obciążeniu: procesorów, pamięci RAM, IO,
 - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:

	▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. • Serwer musi posiadać deklarację CE. • 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.
Warunki gwarancji	- Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. - 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 / 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 zgłoszenia 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 autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
--	--

3. NAS I – 2 sztuki

Minimalne wymagania Zamawiającego:	
Procesor	Procesor 64 bit x86 o taktowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 16GB
Pamięć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 4 zatoki 3,5"
Obsługiwane dyski	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD
Wbudowane w urządzenie interfejsy na dyski M2	Wymagane min. 2 x M2 PCIe Gen3x1
Możliwość stosowania dysków twardych o pojemności	do 18TB
Zainstalowane dyski	4x 10 TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Diody LED	Minimum Status, LAN, HDD
Porty USB 3.2 Gen2	Minimum 3
Port PCIe	Tak, minimum 2 Gen3x4
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Max. 250 W
Oprogramowanie:	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Agregacja łączy	Tak

Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP)

	Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	3 lata

4. NAS II – 1 sztuka

Minimalne wymagania Zamawiającego:	
Procesor	Procesor 64 bit x86 o taktowaniu minimum 2,5Ghz
Procesor liczba rdzeni	Nie mniej niż 6
Pamięć RAM	Nie mniej niż 32GB DDR4
Pamięć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 6

Obsługiwane dyski twarde	3.5" SATA oraz 2.5" SATA oraz 2.5" SATA SSD
Pojemność dysków twardych	do 24TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2 Gen 2	Minimum 3
Port PCIe	Tak, minimum 2
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Max. 250 W
Specyfikacja oprogramowania:	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Wymagania dla systemu operacyjnego opartego o system plików EXT4:	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci

	Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.

Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	3 lata

5. Dyski twarde do NAS – 6 sztuk

Minimalne wymagania:	
Pojemność	min. 16000 GB
Typ	HDD (magnetyczny)
Format	Format 3,5 cala
Interfejs	SATA III (6.0 Gb/s)
Pamięć cache	min. 512 MB
Prędkość obrotowa	7200 obr./ min.
Prędkość odczytu (maksymalna)	do 259 MB/s
Technologia	CMR
Niezawodność MTBF	do 2 500 000 godzin

6. UPS I – 3 sztuki

Minimalne wymagania Zamawiającego:	
Minimalne wymagania techniczne dla jednostki UPS	- Moc znamionowa jednostki nie mniej niż 1.5kW / 1.5kVA - Montaż w szafie rack - Technologia Podwójnej konwersji (online) - Klasa VFI-SS-111 zgodnie z PN-EN62040-1 - Temperatura eksploatacji 0 - 40 °C - Wilgotność względna podczas pracy 0 - 95 % - Wysokość n.p.m. podczas pracy 0-3000metry - Hałas słyszalny w odległości 1 m od powierzchni urządzenia 50.0dBA - Rozpraszanie ciepła w trybie online 317.0BTU/godz - Klasa ochrony IP 20 - Klasa energetyczna sprzętu przeciwprzepięciowego 432J
Parametry wejściowe	- Nominalne napięcie wejściowe 230V - Częstotliwość wejściowa 40–70 Hz (wykrywanie automatyczne) - Typ gniazda wejściowego: - British BS1363A, - IEC-320 C14,

	- Schuko CEE 7/EU1-16P • Zakres napięcia wejściowego w trybie podstawowym 50-150 (połowa obciążenia), 80-150V (pełne obciążenie) • Inne napięcia wejściowe 220, 240
Parametry wyjściowe	Napięcie wyjściowe 230V • Zniekształcenia napięcia wyjściowego $\leq 2\%$ • Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ± 3 Hz • Inne napięcia wyjściowe 220, 240 • Współczynnik szczytu 3: 1 • Typ przebiegu sinusoida • Złącza/gniazda wyjściowe (6) IEC 320 C13 • Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny • Czas autonomii: 5 minut 12 sekund dla pełnego obciążenia 14 minut 12 sekund dla połowy obciążenia • Typowy czas ładowania 3 godziny • Oczekiwana żywotność akumulatora (lata) 3 – 5 • Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów • Baterie wymieniane na gorąco • Opcje przedłużonego podtrzymania zasilania: do 10 zewnętrznych modułów bateryjnych
Komunikacja i zarządzanie	• Gniazdo do montażu karty WEB/SNMP- Smart Slot x1 • Porty komunikacyjne: RJ45, Smart-Slot, USB • Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD • Alarm dźwiękowy Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia • Awaryjny wyłącznik zasilania (EPO)- Tak
Certyfikaty, zgodności oraz gwarancja	• CE, EAC, RoHS • 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulatory
Oprogramowanie	• Dostępne oprogramowanie do zarządzania/monitoringu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.
Dodatkowe informacje	• Automatyczne włączenie UPS-a po powrocie zasilania • Automatyczny test

Zasilacz UPS musi być wyposażony w sterowane programowo gniazda wyjściowe (co najmniej dwie grupy gniazd). Sterowanie gniazd musi umożliwiać sekwencyjne wyłączanie / załączanie odbiorów w zaprogramowanym interwale czasowym. Sterowanie gniazdami musi umożliwiać również powiązanie ze zdarzeniami.

Wyświetlacz LCD musi sygnalizować obsłudze stany ostrzegawcze i alarmowe poprzez zmianę koloru podświetlenia ekranu: ostrzeżenie – kolor pomarańczowy, stan alarmowy – kolor czerwony (podświetlenie pulsujące).

7. UPS II – 1 sztuka

Minimalne wymagania Zamawiającego:	
Minimalne wymagania techniczne dla jednostki UPS	Moc znamionowa jednostki nie mniej niż 1000W / 1.5kVA Montowany w szafie RACK z kompletem uchwytów Technologia Line Interactive Temperatura eksploatacji 0 - 40 °C • Wilgotność względna podczas pracy 0 - 95 % • Wysokość n.p.m. podczas pracy 0-3000 m • Hałas słyszalny w odległości 1 m od powierzchni urządzenia 45.0dBA • Rozpraszanie ciepła w trybie online 135.0BTU/godz. • Klasa energetyczna sprzętu przeciwprzepięciowego 459 Dżule
Parametry wejściowe	• Nominalne napięcie wejściowe 230V • Częstotliwość wejściowa 47/63 Hz +/- 3 Hz (automatyczne wykrywanie) • Typ gniazda wejściowego: IEC-320 C14 • Zmienny zakres napięcia wejściowego w trybie podstawowym 170 - 300V • Inne napięcia wejściowe 220, 240
Parametry wyjściowe	• Napięcie wyjściowe 230V • Zniekształcenia napięcia wyjściowego poniżej 5% • Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 47/63Hz +/- 3 Hz • Inne napięcia wyjściowe 220, 240 • Typ przebiegu sinusoida • Złącza/gniazda wyjściowe (8) IEC 320 C13 (Zasilanie zapasowe) (2) IEC Jumpers (Zasilanie zapasowe)
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu • Czas autonomii: 6 minut 30 sekund dla pełnego obciążenia 23 minuty 4 sekundy dla połowy obciążenia • Typowy czas ładowania 3 godziny • Oczekiwana żywotność akumulatora (lata) 4 – 6 • Baterie wymieniane na gorąco
Komunikacja i zarządzanie	• Porty komunikacyjne: RJ-45 Serial, USB, Smart Slot • Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD Alarm dźwiękowy: Alarm przy zasilaniu z akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia
Certyfikaty, zgodności oraz gwarancja	• Znak C, CE, CSA, GOST, UL 1778, VDE, RoHS, REACH • 2 lata na naprawę lub wymianę
Oprogramowanie	• Dostępne oprogramowanie do zarządzania/monitoringu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.

	• Oprogramowanie do zarządzania zasilaczami UPS do bezpiecznego wyłączenia i zarządzania energią dla komputerów stacjonarnych, serwerów i stacji roboczych, wykorzystujące dedykowane połączenia szeregowo lub USB i oferujące: ○ Monitorowania i zarządzania zasilaczy UPS ○ Bezobsługowego, bezpiecznego wyłączenia podczas problemów z zasilaniem ○ Bezpieczny dostęp do internetowego interfejsu użytkownika (UI) ○ Możliwość dokładnego określania czasu i sekwencji zdarzeń powodujących zdarzenie za pomocą dziennika zdarzeń ○ Identyfikacja potencjalnie niebezpiecznych trendów zanim dojdzie do eskalacji problemu lub eksportowanie dziennika w celu analizy
Dodatkowe informacje urządzenia	• możliwość zimnego startu • automatyczny test akumulatora • automatyczne włączenie UPS-a po powrocie zasilania

8. Zarządzalne urządzenia sieciowe z obsługą VLAN – 3 sztuki

Cechy sprzętowe:

- Urządzenie musi być wyposażone w min. 24 portów RJ45 2,5Gbps oraz min. 4 porty SFP+
- Porty RJ45 muszą być wstecznie kompatybilne z niższymi prędkościami 10/100/1000Mbps
- Porty SFP+ muszą obsługiwać wkładki o prędkości zarówno 1Gbps jak i 10Gbps
- Urządzenie musi być wyposażone w port konsoli umożliwiający zarządzanie urządzeniem z poziomu linii komend
- Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward
- Rozmiar tablicy adresów MAC urządzenia min. 32K
- Rozmiar bufora – min 16 MB
- Min. przepustowość urządzenia – 200 Gbps
- Min. szybkość przekierowań pakietów – 148,80 Mpps
- Urządzenie musi wspierać funkcjonalność PoE zgodną ze standardem 802.3af/at, minimalny wymagany budżet dostępny dla zasilanych urządzeń to 500W
- Maksymalny pobór mocy urządzenia nie może przekraczać 650W
- Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19" oraz posiadać w zestawie odpowiednie uchwyty montażowe
- Głębokość urządzenia nie może przekraczać 340 mm

Standardy:

Urządzenie musi spełniać następujące standardy:

- 802.3i
- 802.3u
- 802.3z
- 802.3ae
- 802.3ab
- 802.3x

na Rozwój Cyfrowy

- 802.3az
- 802.3ad
- 802.3af
- 802.3at
- 802.3bz
- 802.1ab
- 802.1D
- 802.1w
- 802.1s
- 802.1p
- 802.1q

Funkcjonalność:

Wymaga się, aby urządzenie posiadało następujące funkcjonalności:

- Zarządzanie za pomocą przeglądarki poprzez interfejs http/https
- Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa pełna konfiguracja urządzenia
- Urządzenie musi mieć obsługiwać możliwość adopcji przez zewnętrzny kontroler w celu scentralizowanego zarządzania
- Obsługę stosu IPv4 i IPv6
- Funkcję wykrywania pętli
- Funkcję izolacji portów
- Możliwość włączenia lub wyłączenia zasilania PoE na danym porcie
- Funkcję agregacji portów z wykorzystaniem protokołu LACP
- Obsługę protokołu LLDP/LLDP-MED
- Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6
- Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6)
- Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP)
- Obsługę 4K identyfikatorów VLAN
- Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN)
- IGMP Snooping oraz MLD Snooping
- Obsługę min. 500 grup multicastowych jednocześnie
- MVR
- Obsługę routingu statycznego i/lub dynamicznego
- Możliwość konfiguracji co najmniej 16 interfejsów IP
- Obsługę min. 40 tras statycznych dla funkcji routingu statycznego
- Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+
- Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia
- Obsługę list kontroli dostępu (ACL)
- Obsługę SNMP w wersjach v1/v2c/v3
- Obsługę grup RMON 1,2,3,9)

Pozostałe wymagania:

- Urządzenie musi posiadać certyfikację CE

- Gwarancja na urządzenie musi wynosić min. 5 lat
- Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego producenta
- Urządzenie musi być zarządzane przez SDN Omada ze względu na konieczność utrzymania jednakowego systemu.

9. UTM – 1 sztuka

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
 - 5 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregową oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.

4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

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

- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPsec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPsec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPsec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
 - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

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

Ochrona przed atakami

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

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

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

Zarządzanie

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

Logowanie

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

Testy wydajnościowe oraz funkcjonalne

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

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

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

10. Licencje UTM – 1 sztuka

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres nieprzekraczający 30.06.2026 roku.

11. Licencje UTM – 1 sztuka

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres nieprzekraczający 30.06.2026 roku.

12. Oprogramowanie do monitorowania infrastruktury informatycznej – 80 licencji wieczystych

Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych

Oprogramowanie musi spełniać następujące wymagania w zakresie zarządzania zasobami IT:

- Zarządza wszystkimi zasobami, za które odpowiada dział IT.
- Pokazuje szczegółowe informacje i ewidencję czynności wykonanych na zasobach w trakcie całego cyklu życia.
- Ma możliwość definiowania statusów i pól oraz generowanie protokołu przekazania sprzętu.
- Potrafi przypisać dokument do wielu zasobów.
- Generuje dokumenty na podstawie szablonów.
- Automatycznie numeruje dodawane zasoby i dokumenty według zdefiniowanego wzorca numeracji.
- Posiada system zarządzania aplikacjami i licencjami.
- System identyfikuje realne zużycie licencji.
- Rozlicza licencje według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji.

- Posiada historię użycia konkretnych licencji oprogramowania.
- Oprogramowanie robi audyt inwentaryzacji sprzętu i oprogramowania.
- Posiada zdalny dostęp do menadżera plików z możliwością usuwania plików użytkownika.
- System zbiera informacje o wpisach rejestrowych, plikach, archiwach oraz konfiguracji sprzętowej konkretnych stacji roboczych.
- Zarządza instalacjami/dezinstalacjami oprogramowania w oparciu o menadżera pakietów MSI.
- Ma możliwość archiwizacji i porównywania audytów.
- Monitoruje harmonogram zadań Windows.

Oprogramowanie musi spełniać następujące wymagania w zakresie zarządzania użytkownikami:

- Zarządza użytkownikami, bazując na grupach i politykach bezpieczeństwa.
- Przyporządkowuje dane do konkretnego użytkownika.
- Blokuje niebezpieczne domeny WWW.
- Chroni pracowników przed wiadomościami phishingowymi i atakami APT.
- Rozróżnia wykonywane czynności na poszczególnych urządzeniach.
- Posiada rejestr naruszeń blokad, który agreguje informacje o próbach dostępu do blokowanych stron.
- Posiada dedykowane alarmy dla wszystkich rodzajów incydentów zbieranych przez rejestr naruszeń blokad.
- Ma możliwość blokowania uruchamianych aplikacji.
- Może korzystać z zewnętrznych list blokowania stron takich jak listę ostrzeżeń CERT.PL
- Monitoruje wiadomości e-mail.
- Zbiera informacje o odwiedzanych stronach WWW.
- Monitoruje użycie łącza przez poszczególnych użytkowników.
- Zarządza regułami blokowania aplikacji i stron WWW.
- Ma możliwość wykrywania podejrzanych aktywności użytkowników za pomocą mechanizmu wykrywania jigglerów.

Oprogramowanie musi spełniać następujące wymagania w zakresie pomocy technicznej:

- Posiada tworzenie zgłoszeń serwisowych i zarządza nimi.
- Ma możliwość wskazania osób, które muszą zaakceptować zgłoszenie.
- Tworzy ścieżki akceptacji na podstawie kategorii przypisanej do zgłoszenia.
- Posiada możliwość stworzenia listy aplikacji bezpiecznych do samodzielnej instalacji przez użytkownika.
- Może przetwarzać zgłoszenia w trybie anonimowym.
- Posiada rozbudowany system raportów.
- Ma bazę zgłoszeń z rozbudowaną wyszukiwarką.
- Posiada wewnętrzny komunikator z możliwością przesyłania plików oraz przydzielania uprawnień.
- Oprogramowanie posiada zdalny dostęp do komputerów z możliwością blokowania myszy/klawiatury.
- Ma równoczesny zdalny dostęp kilku administratorów do jednego agenta.
- Posiada integrację bazy użytkowników z Active Directory.
- Zarządza kontami lokalnych użytkowników Windows.

Oprogramowanie musi spełniać następujące wymagania w zakresie kontroli dostępu do danych:

- Automatycznie nadaje użytkownikom domyślną politykę monitorowania i bezpieczeństwa.
- Monitoruje operacje na plikach z zasobów sieciowych udostępnianych przez urządzenia.
- Zabezpiecza sieć przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych.
- Posiada integrację z Windows Defender, Windows Firewall i Windows Bitlocker.
- Alarmy o podłączonym urządzeniu obcym.
- Możliwość zdalnego szyfrowania dysków.

- Zbiera informacje o urządzeniach podłączonych do danego komputera.
- Posiada bazę wszystkich urządzeń podłączonych do komputerów w sieci.
- Posiada historię połączeń i operacji na urządzeniach przenośnych.
- Zarządza prawami dostępu.
- Ustawia reguły dla całej sieci.

Oprogramowanie musi spełniać następujące wymagania w zakresie zarządzania czasem:

- Posiada statystyki czasu spędzonego przed komputerem.
- Ma możliwość tworzenia grup złożonych z dowolnych pracowników w firmie.
- Posiada listę aplikacji używanych przez poszczególnych pracowników.
- Dodawanie dostępu do odpowiednich aplikacji dla danych grup pracowników.
- Możliwość oznaczania stron internetowych i aplikacji jako produktywnie, neutralne lub nieproduktywne.
- Posiada listę kontaktów w danej organizacji.
- Podgląd zrzutu ekranu wybranego użytkownika dostępny dla menadżerów i administratorów.

13. Oprogramowanie antywirusowe – 50 licencji

Odnowienie licencji dla posiadanego oprogramowania ESET Essential na okres nieprzekraczający 30.06.2026 roku.

Administracja zdalna

1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
8. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
9. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
10. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
11. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

12. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
13. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
14. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
15. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

Ochrona stacji roboczych

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

- c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
 17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
 18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
 19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
 20. Rozwiązanie musi posiadać funkcjonalność skanera EFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera EFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci

masowych Firewall, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji,
 - a. nazwę pakietu,
 - b. kategorię sklepu Google Play,
 - c. uprawnienia aplikacji,
 - d. pochodzenie aplikacji z nieznanego źródła.

14. Oprogramowanie antywirusowe – 40 licencji

na okres nieprzekraczający 30.06.2026 roku.

Administracja zdalna

2. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
3. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.

4. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
5. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
6. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
7. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne –jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - b. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - c. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - d. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - e. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - f. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne –jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego

z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonych mikro-serwisu.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji,
 - b. nazwę pakietu,
 - c. kategorię sklepu Google Play,
 - d. uprawnienia aplikacji,
 - e. pochodzenie aplikacji z nieznanego źródła.

15. Wsparcie lokalne przy wdrożeniu – 1 sztuka

Usługi wdrożeniowe realizowane będą hybrydowo, częściowo w siedzibie Zamawiającego, częściowo przy pomocy zdalnego połączenia z systemami Zamawiającego.

CZĘŚĆ II

1. Testy penetracyjne – 3 sztuki

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);
- weryfikację 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 celu 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 (offensive 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 skanowań 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 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. Eksploatacja.
 1. Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force.
 2. Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji).
 3. Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, błędy w konfiguracji serwera www, błędy architektury aplikacji internetowych, innych wystawionych publicznie 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. Listę danych zebranych w trakcie rekonesansu.
4. Listę znalezionych podatności wraz z określoną dla niej wagą zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.
5. Szczegółowy opis znalezionych podatności.
6. Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.

2. Szkolenie z cyberbezpieczeństwa dla pracowników – 1 sztuka

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 od 6 do 8 godzin roboczych, rozłożonych na co najmniej 1 dzień.

Zajęcia będą organizowane w dwóch 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. Opracowanie i wdrożenie dokumentacji SZBI – 3 sztuki

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 opracowywania i ustanawiania, wdrażania i eksploatacji, monitorowania i przeglądu oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego 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 osiągnięcia 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 domniemych 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 Informatycznych

- Procedura Instalacji i Konfiguracji Systemów Informatycznych 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 Informatycznych

- Procedura Użytkowania Systemów Informatycznych musi definiować zasady korzystania z systemów informatycznych 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 użytkownika 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 wyłączenia 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 nieznanymi 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 III

1. Agregat – 1 sztuka

Agregat wykonany zgodnie z obowiązującymi normami i standardami:

- 2006/42/WE Dyrektywa Maszynowa
- Kompatybilność elektromagnetyczna 2014/30/UE.
- 2014/35/UE sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia

PN-EN ISO 8528-13:2016-07

PN- EN ISO 3744:2011

ISO 8528-1:2005

2000/14/WE, 2005/88/WE – Dyrektywa Hałasowa

Klasa wykonania minimum G2.

Wymagane jest aby agregat pochodził z seryjnej i bieżącej produkcji.

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) dokumentacja w języku polskim,
- c) Uruchomienie agregatu (paliwo na czas rozruchu zapewnia wykonawca),
- d) gwarancja 60 miesięcy z limitem 1000 mth.,
- e) dostawca musi posiadać autoryzację do obsługi serwisowej silnika oraz prądnicy (ASO – Autoryzowana Stacja Obsługi),
- f) obecność Producenta marki na rynku w Polsce powyżej 10 lat (sprzedaż, serwis, magazyn części),
- g) 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 Rzeczypospolitej Polskiej, pochodzą z oficjalnego, autoryzowanego kanału sprzedaży na rynek polski, posiadają serwis i wsparcie producenta.

Agregat w wersji obudowanej.

Wymagana moc znamionowa agregatu min. – 50 kVA (40 kW).

Wymagana moc awaryjna agregatu min. – 55 kVA (44 kW).

Napięcie – 400/230 V.

Częstotliwość – 50Hz.

Powinien być wyprodukowany w Polsce i posiadać oznaczenie CE.

Dostarczone urządzenie powinno być wytworzone przez jednego producenta posiadającego:

- wdrożony system ISO 9001:2015,
- wdrożony system AQAP 2110:2016

Obudowa dźwiękochłonna, wyciszona specjalną, niepalną pianką wygłuszającą, z niezbędnymi drzwiami dostępowymi na dłuższych bokach.

Wylot spalin i gorącego powietrza poprzez górną połąć obudowy.

Podejście kablowe umiejscowione na dłuższym boku po lewej stronie, bezpośrednio pod wyłącznikiem głównym agregatu, umożliwiające wprowadzenie okablowania bez wychodzenia kablami poza obrys agregatu.

Mocna konstrukcja z możliwością transportu wózkami widłowym, dźwigiem, HDS – na pasach, widłach lub łańcuchach.

Rama izolowana od podłoża za pomocą stóp przykręconych do ramy, z możliwością regulacji wysokości (poziomowania).

Zewnętrzny przycisk zatrzymania awaryjnego.

Zaciski na listwie sterowniczej:

- styk NC do podłączenia okablowania zewnętrznego stopu pożarowego
- dla podłączenia okablowania potrzeb własnych agregatu.
- dla podłączenia okablowania sterowania układem SZR.

Wysokowydajne amortyzatory drgań silnika i prądnicy.

Wymiary nie przekraczające (dł. x szer. x wys.) – 1900 x 1000 x 1250 [mm]

Zbiornik paliwa co najmniej 100 L w ramie agregatu, pozwalający na ciągłą pracę agregatu:

- przy 75% obciążeniu co najmniej, 12 h
- przy 100% obciążeniu co najmniej, 8 h.

Pojemnościowy czujnik poziomu paliwa z % wskazaniem poziomu na sterowniku

Alarm poziomu paliwa

Wyłączenie agregatu przy 5% paliwa (zabezpieczenie przed zapowietrzeniem)

Wymagany również korek spustowy zbiornika oraz co najmniej jeden niezależny, otwór w zbiorniku zaślepiony deklek na śrubach, umożliwiający montaż i podłączenie dodatkowej instalacji paliwowej, lub przeniesienie wlewu paliwa na drugą stronę zbiornika.

Stalowy tłumik dźwięków -35db(A) – zabudowany wewnątrz agregatu

Liczba i układ cylindrów – 4 L.

Wymagany typ wtrysku – bezpośredni.

Elektroniczna regulacja obrotów.

Emisja spalin - non emission

Podgrzewanie bloku – grzałka silnika kontrolowana przez sterownik agregatu.

Spalanie przy 75% obciążenia nie więcej niż – 8,0 l/h.

Spalanie przy 100% obciążenia nie więcej niż – 12,0 l/h.

Wlew paliwa - korek zamykany kluczykiem, wewnątrz obudowy.

Filtr powietrza suchy.

Silnik chłodzony glikolem.

Prędkość obrotowa – 1500 r.p.m.

Układ elektryczny 12V lub 24V.

Akumulator 12V (lub 2x12V)

Automatyczna ładowarka buforowa akumulatora/ów 12V lub 24V/5A w czasie czuwania.

Ośłona elementów gorących oraz ruchomych.

Prądnica wyposażona w automatyczną regulację napięcia

Obudowa (wg IEC-34-5) - IP23.

Złącze – elastyczny dysk.

Klasa izolacji – H.

Sterownik LCD z menu w j. polskim, pozwalający na kontrolę parametrów sieci i agregatu (napięcie, prądów, mocy, częstotliwości, cos ϕ , napięcia ładowania akumulatora, ilość paliwa w zbiorniku, czasu pracy agregatu, parametrów silnika).

Panel sterownika wyposażony w tabliczkę z diodami sygnalizacyjnymi dla łatwej obsługi i szybkiej identyfikacji stanów pracy urządzenia. Wymagana jest identyfikacja alarmów dotyczących działania baterii, pracy alternatora, poziomu paliwa, ciśnienia oleju oraz dwa dodatkowe do zdefiniowania. Sterownik musi posiadać w tylnej ścianie wolne sloty do podłączenia dodatkowych modułów sygnalizacyjnych np. GSM, ETHERNET, styków/wyjść przekaźnikowych dla sygnałów bezpotencjałowych (do zdefiniowania przez użytkownika)

Funkcje i wyposażenie sterownika LCD:

- Obsługa 400 Hz
- Dziennik - 400 zdarzeń,
- Możliwość edycji wszystkich parametrów na panelu przednim
- 3-poziomowe hasło konfiguracyjne
- Graficzny wyświetlacz LCD
- Wyświetlanie przebiegów napięcia i prądów
- Analiza harmoniczných

na Rozwój Cyfrowy

- Wyjścia 16 A MCB i GCB
- 8 konfigurowalnych wejść cyfrowych
- Wejścia rozszerzalne do 40
- 6 konfigurowalnych wyjść cyfrowych
- Wyjścia z możliwością rozszerzenia do 38
- 3 konfigurowalne wejścia analogowe
- 3 konfigurowalne alarmy serwisowe
- Tygodniowy harmonogram pracy
- Ręczna „precyzyjna regulacja prędkości” w wybranych ECU
- Automatyczne sterowanie pompą paliwa
- Ochrona przed nadmierną mocą
- Odwrotna ochrona zasilania
- Zabezpieczenie przed przeciążeniem IDMT
- Zrzut obciążenia, obciążenie zastępcze
- Zarządzanie wieloma obciążeniami
- Zabezpieczenie od asymetrii prądu
- Ochrona przed asymetrią napięcia
- Zegar czasu rzeczywistego z podtrzymaniem baterijnym
- Kontrola prędkości biegu jałowego
- Ładowanie akumulatora włączone
- Wiele parametrów nominalnych
- Napęd Tactor i MCB
- 4 kwadrantowe liczniki mocy agregatu
- Liczniki zasilania sieciowego
- Wskazania poziomu paliwa
- Wyświetlacz diagnostyczny modemu
- Konfigurowalny przez USB, RS-485 i GPRS

Funkcje pomiarowe sterownika

- Napięcia sieci i agregatu PN / PP
- Częstotliwość sieci i agregatu
- Prądy fazowe sieci i agregatu
- Prądy neutralne sieci i agregatu
- Sieć i agregat, faza i suma, kW, kVA, kVAr, pf
- Prędkość silnika
- Napięcie baterii
- Temperatura silnika
- Ciśnienie oleju
- Zużycie paliwa (dla silników wyposażonych w ECU)

KOMUNIKACJA

- 4-pasmowy modem GPRSwbudowany lub z możliwością rozszerzenia,
- Port USB
- RS-485 (2400-115200).....wbudowany lub z możliwością rozszerzenia,
- RS-232 (2400-115200)
- J1939-CANBUS
- Centralny monitoring internetowy
- Wysyłanie wiadomości SMS...opcjonalnie
- Wysyłanie e-mail...wbudowany lub z możliwością rozszerzenia,
- Darmowe oprogramowanie na PC: Rainbow Plus

- Modbus RTU

Dodatkowe gniazda odbioru mocy agregatu:

Zamawiający wymaga aby na agregacie zamontowane były dodatkowe gniazda zasilające:

- min 1 szt. x gniazdo pełnego odbioru mocy z agregatu
- min 1 szt. x gniazdo 32A /400V
- min 2 szt. x gniazda 16A / 230V

Zabezpieczone według obowiązujących norm i przepisów.

Przyczepa transportowa

Zamawiający wymaga również aby Wykonawca dostarczył do siedziby zamawiającego przyczepę nie będącą integralną częścią agregatu prądotwórczego.

Dane techniczne przyczepy transportowej :

- Wymiary platformy ładunkowej- ok. 2,40m x1,3m
- 1 Oś firmy KNOTT lub AL-KO KOBER (lub równoważna) o nośności 1350kg
- Koła na zewnątrz ramy
- Urządzenie najazdowe z hamulcem ręcznym postojowym i zaczepem kulowym
- Koła 175R14C- 2szt.
- dyszel o stałej wysokości sprzęgu z zaczepem kulowym
- podłoga sklejk wodoodporna z warstwą antypoślizgową grubość 12mm
- błotniki metalowe, zaślepione od wewnątrz
- konstrukcja ramy wykonana z elementów stalowych – cynkowana ogniowo
- rama przystosowana pod montaż agregatu (wzmocnienia wzdłużne całości przyczepy)
- 4 podpory rurowe stabilizujące po bokach
- koło manewrowe z przodu
- kliny pod koła – 2sz
- oświetlenie zgodne z PN z wtyczka 13 PIN

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

CPV 48820000-2 serwery

CPV 48000000-8 pakiety oprogramowania i systemy informatyczne

CPV 79212000-3 usługi audytu

CPV 80550000-4 usługi szkolenia w dziedzinie bezpieczeństwa

CPV 72710000-0 usługi w zakresie lokalnej sieci komputerowej

CPV 72263000-6 usługi wdrażania oprogramowania

CPV 72268000-1 usługi dostawy oprogramowania

CPV 31122000-7 Jednostki prądotwórcze

VI Miejsce i Terminy wykonania zamówienia

Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Dostawy sprzętu oraz oprogramowania z części I będą realizowane w ciągu 30 dni od dnia podpisania umowy, wdrożenia i szkolenia z części II będą realizowane w ciągu 120 dni od dnia podpisania umowy/ lub zgodnie z wskazaniem Wykonawcy przy uwzględnieniu kryteriów w części II zamówienia/, dostawa sprzętu z części III będzie realizowana w ciągu 30 dni od dnia podpisania umowy.

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

VII 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. Do części I zamówienia - Na potwierdzenie spełnienia warunku udziału w postępowaniu, dotyczącego zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca wykazał się odpowiednim doświadczeniem, tj. w ciągu ostatnich 3 lat przed upływem terminu składania ofert, w tym okresie realizuje, bądź zrealizował należycie co najmniej jedną dostawę/ usługę w zakresie dostawy sprzętu komputerowego na kwotę co najmniej 300 000 złotych brutto.
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.

VIII Przestanki 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).

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

1. Obowiązek określony powyżej dotyczy również podwykonawców.
2. 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.
3. Pozostałe osoby uczestniczące w wykonaniu zamówienia mogą współpracować z Wykonawcą na podstawie umów cywilnoprawnych.
4. W przypadku uzasadnionych wątpliwości co do przestrzegania prawa pracy przez Wykonawcę lub Podwykonawcę, Zamawiający może zwrócić się o przeprowadzenie kontroli przez Państwową Inspekcję Pracy.

X 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:
 - Do części I zamówienia - 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 dostawy/ usługi zostały wykonane, przed upływem terminu składania ofert, w co najmniej jednej dostawy/usługi usług w zakresie dostawy sprzętu komputerowego na kwotę co najmniej 300 000 złotych brutto 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 II 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 II zamówienia - ITIL® Foundation Certificate in IT Service Management w zakresie projektowania, zrozumienia i zastosowania najlepszych praktyk w zarządzaniu usługami informatycznymi;
 - do części II 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.

XI Poleganie na zasobach podmiotów trzecich

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.

XII Podwykonawstwo

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom):
2. Zamawiający **nie zastrzega** obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.

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 jakiegokolwiek 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 **25 czerwca 2025 r. do godz. 10 00 /środa/** za pośrednictwem platformazakupowa.pl pod adresem: <https://platformazakupowa.pl/1121252>
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.
4. Otwarcie ofert nastąpi **25 czerwca 2025 r. o godz. 10 30** poprzez platformę zakupową.
5. Wykonawca nie może wprowadzić zmian do złożonej oferty.
6. 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

Do części I zamówienia:

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

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	100

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 100% (maksymalnie do 100 pkt)
- Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
- Punkty w kryterium „Cena” będą obliczane na podstawie wzoru:

$$C = CC_{\min} / CC_{\text{of}} \times 100$$

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

6. 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.

Do części II zamówienia:

Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	90
2.	Termin realizacji wdrożeń	10

1. Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.

2. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.

3. 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:

$$C = CC \min / CC of \times 90$$

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.

4. Kryterium „Termin realizacji wdrożeń” stanowi maksymalnie do 10 pkt przy kryteriach:

- Do 120 dni – 0 pkt;
- Do 90 dni – 5 pkt;
- Do 60 dni – 10 pkt;

5. 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 „Termin realizacji wdrożeń”,

Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku

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

7. 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.

Do części III zamówienia:

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

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	100

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 100% (maksymalnie do 100 pkt)
- Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
- Punkty w kryterium „Cena” będą obliczane na podstawie wzoru:

$$C = CC_{\min} / CC_{\text{of}} \times 100$$

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

6. 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. Wzór Umowy dla części I stanowi Załącznik nr 2.1 do SWZ.
2. Wzór Umowy dla części II stanowi Załącznik nr 2.2 do SWZ.
3. Wzór Umowy dla części III stanowi Załącznik nr 2.3 do SWZ.

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 04.05.2016, str. 1), dalej „RODO”, informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Gmina Sępólno ul. 11 Listopada 7, 11-210 Sępólno, e-mail: sepopol@sepopol.pl
2. Jeżeli ma Pani/Pan pytania dotyczące sposobu i zakresu przetwarzania Pani/Pana danych osobowych w związku z udzieleniem lub wykonywaniem zamówienia publicznego, a także przysługujących Pani/Panu uprawnień, może Pani/Pan skontaktować się z Inspektorem Ochrony Danych Gmina Sępólno ul. 11 Listopada 7, 11-210 Sępólno, e-mail: jod@jgconsulting.net.pl
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie niniejszego zamówienia publicznego.
4. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania na podstawie przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. 2024 r. poz. 1320).
5. Pani/Pana dane osobowe będą przechowywane, 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 oraz w celu archiwizacji.

6. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp.
7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO.
8. Posiada Pani/Pan:
- 1) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - 2) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
 - 3) 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;
 - 4) 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:
- 1) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - 2) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - 3) 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. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym, a Wykonawcami odbywała się będzie za pośrednictwem Systemu platformy zakupowej - zwanego dalej Platformą dostępnego pod adresem <https://platformazakupowa.pl/transakcja/1121252>
2. Wszelkie informacje dotyczące postępowania w tym zapytania i odpowiedzi dla Wykonawców, modyfikacje SWZ, ogłoszenie wyników itp., będą zamieszczane na Platformie.
3. Przed przystąpieniem do składania oferty, Wykonawca jest zobowiązany zapoznać się z Instrukcją dla wykonawców pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>.
4. W postępowaniu o udzielenie zamówienia komunikacja pomiędzy Zamawiającym a Wykonawcami, w szczególności składanie oświadczeń, wniosków (innych niż o dopuszczenie do udziału w postępowaniu), zawiadomień oraz przekazywanie informacji, odbywa się elektronicznie za pośrednictwem dedykowanych funkcji formularzy „Wiadomość” dostępnych dla każdego zalogowanego Wykonawcy.
5. Wszelką korespondencję związaną z niniejszym postępowaniem, należy przekazywać za pośrednictwem Systemu e-ZP. Korespondencję uważa się za przekazaną w terminie, jeżeli dotrze do Zamawiającego przed upływem wymaganego terminu. Każda ze stron na żądanie drugiej niezwłocznie potwierdzi fakt otrzymania wiadomości elektronicznej.
6. Zamawiający wyznacza następującą osobę do kontaktu z Wykonawcami:
 - w zakresie postępowania:
Beata Pakuła za pośrednictwem Platformy zakupowej,

7. Specyfikacja połączenia, formatu przesyłanych danych oraz kodowania i oznaczania czasu odbioru danych Systemu Platformy :
- 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.
8. 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).
9. Sposób sporządzenia dokumentów elektronicznych musi być zgodny 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).
10. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienia dotyczące wszelkich wątpliwości związanych z SWZ, przedmiotem zamówienia, sposobem przygotowania i złożenia oferty.
11. Zamawiający udzieli wyjaśnień zgodnie z art. 284 ustawy Pzp.

12. Zamawiający umieści wyjaśnienia w Systemie e-ZP bez ujawnienia źródeł zapytania. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ.
13. 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.
14. Do oferty należy dołączyć oświadczenie o niepodleganiu wykluczeniu, spełnianiu warunków udziału
15. w postępowaniu, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, a następnie zaszyfrować wraz z plikami stanowiącymi ofertę.
16. Oferta może być złożona tylko do upływu terminu składania ofert.
17. Wykonawca może przed upływem terminu do składania ofert wycofać ofertę.
18. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

XX Sposób obliczenia ceny

1. Wykonawca podaje 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 podaje 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 umowę 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 umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertę.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie po-informowany 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.
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 zamieścić w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo

b) zamieścić 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.

XXIII ZAŁĄCZNIKI

Załącznik nr 1 Formularz oferty

Załącznik nr 2.1 Istotne Postanowienia Umowy dla części I

Załącznik nr 2.2 Istotne Postanowienia Umowy dla części II

Załącznik nr 2.3 Istotne Postanowienia Umowy dla części III

Załącznik nr 3 Oświadczenie wykonawcy

Załącznik nr 4 Oświadczenie o braku powiązań osobowych i kapitałowych

Załącznik nr 5 RODO Pozyskiwanie ofert na usługi dostawy roboty - wykonawcy

Załącznik nr 6 RODO Pozyskiwanie ofert na usługi dostawy roboty - reprezentanci wykonawcy

Załącznik nr 7 Wykaz dostaw

Załącznik nr 8 Wzór oświadczenia o spełnianiu warunków udziału w postępowaniu