



SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego pn.:

„Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd”
w Gminie Iwkowa 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”

Identyfikator (ID) postępowania na Platformie e-Zamówienia:

ocds-148610-2ceaae00-ab65-4c39-92fc-7d319fb2a97d

Numer sprawy: S.O.O.271.3.2025.PD

Spis treści

| | |
|--|----|
| I ZAMAWIAJĄCY | 4 |
| II Definicje | 6 |
| III Wartość zamówienia..... | 6 |
| IV Opis przedmiotu zamówienia | 7 |
| V Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV) | 56 |
| VI Miejsce i Terminy wykonania zamówienia | 56 |
| VII Warunki udziału w postępowaniu | 57 |
| VIII Przestanki wykluczenia Wykonawcy..... | 58 |
| IX Obowiązek zatrudniania przez wykonawcę osób na podstawie stosunku pracy (art. 95 PZP) | 59 |
| X Wykaz oświadczeń lub dokumentów, jakie mają złożyć wykonawcy w celu wykazania spełniania warunków udziału w postępowaniu oraz niepodlegania wykluczeniu z postępowania | 59 |
| XI Poleganie na zasobach podmiotów trzecich | 61 |
| XII Podwykonawstwo..... | 61 |
| XIII Informacja dla wykonawców polegających na zasobach innych podmiotów, na zasadach określonych w art. 118 ustawy PZP | 62 |
| XIV Kryterium równoważności..... | 62 |

| | |
|---|----|
| XV Opis sposobu składania ofert w postępowaniu | 63 |
| XVI Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem wag tych kryteriów i sposobu oceny ofert..... | 65 |
| XVII Wzór umowy..... | 67 |
| XVIII RODO | 68 |
| 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 oraz informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami | 70 |
| XX Sposób obliczenia ceny | 74 |
| XXI Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego | 75 |
| XXII Środki ochrony prawnej..... | 75 |
| ZAŁĄCZNIKI..... | 79 |

I ZAMAWIAJĄCY

Gmina Iwkowa
32-861 Iwkowa 468
NIP: 8691212363, REGON: 851660720
email: gmina@iwkowa.pl
tel. 146844010

Adres strony internetowej prowadzonego postępowania, na której udostępniane będą zmiany i wyjaśnienia SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia:

platforma E-Zamówienia <https://ezamowienia.gov.pl/pl/>

(link prowadzący bezpośrednio do widoku postępowania na Platformie E-Zamówienia):

<https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-2ceaae00-ab65-4c39-92fc-7d319fb2a97d>

Postępowanie można wyszukać również ze strony głównej Platformy e-Zamówienia (przycisk „Przeglądaj postępowania/konkursy”).

Adres strony internetowej, na której zamieszczona jest tylko informacja o prowadzonym postępowaniu oraz link prowadzący bezpośrednio do widoku postępowania na Platformie

E-Zamówienia: <https://iwkowa.pl/przetargi.html>

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. (tj. Dz.U. z 2024 r. poz. 1320 ze zm.) oraz aktów wykonawczych wydanych na jej podstawie.

Niniejsze postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym bez negocjacji, 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/dostaw, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.

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 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 od dnia upływu terminu składania ofert (włącznie) **do dnia 10.01.2026r., tj. 30 dni**. 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, obowiązaną na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych do jej stosowania. |
| 4. | Wykonawca | należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która oferuje na rynku wykonanie robót budowlanych lub obiektu budowlanego, dostawę produktów lub świadczenie usług lub ubiega się o udzielenie zamówienia, złożyła ofertę lub zawarła umowę w sprawie zamówienia publicznego. |

III Wartość zamówienia

Szacunkowa wartość zamówienia nie przekracza progów unijnych określonych w art. 3 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 – 1 sztuka

| Parametr | Charakterystyka (wymagania minimalne) |
|----------------------------|---|
| Obudowa | <ul style="list-style-type: none"> Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| Płyta główna | <ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| Chipset | <ul style="list-style-type: none"> Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| Procesor | <ul style="list-style-type: none"> Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| RAM | <ul style="list-style-type: none"> Minimum 256GB DDR5 RDIMM 4800MT/s, |
| Funkcjonalność pamięci RAM | <ul style="list-style-type: none"> Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) |

| | |
|-----------------------------------|---|
| Gniazda PCI | <ul style="list-style-type: none"> Min. dwa sloty PCIe |
| Interfejsy sieciowe/FC/SAS | <ul style="list-style-type: none"> Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT Dodatkowa Karta Dual Port (2x SFP+, 10Gb/s, SFP+, PCIe) |
| Dyski twarde | <ul style="list-style-type: none"> Zainstalowane <ul style="list-style-type: none"> 2x dysk SSD SATA o pojemności min. 480GB, 12Gb, 2,5" Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| Kontroler RAID | <ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10 |
| Wbudowane porty | <ul style="list-style-type: none"> 4x USB, w tym min. 1 porty USB 3.0 2x port VGA (jeden na panelu przednim) Możliwość rozbudowy o Serial Port |
| Video | <ul style="list-style-type: none"> Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| Wentylatory | <ul style="list-style-type: none"> Redundantne, Hot-Plug |
| Zasilacze | <ul style="list-style-type: none"> Redundantne, Hot-Plug min. 1100W klasy Titanium |
| Bezpieczeństwo | <ul style="list-style-type: none"> Zatrask górnej pokrywki oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający |

| | |
|--------------------------------------|---|
| | wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| Karta Zarządzania | <ul style="list-style-type: none"> Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: <ul style="list-style-type: none"> 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 <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> 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 |

| | |
|-------------|--|
| | <ul style="list-style-type: none"> Podsumowanie stanu dla każdego urządzenia Szczegółowy status urządzenia/elementu/komponentu Generowanie alertów przy zmianie stanu urządzenia. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń Integracja z service desk producenta dostarczonej platformy sprzętowej Możliwość przejęcia zdalnego pulpitu Możliwość podmontowania wirtualnego napędu Kreator umożliwiający dostosowanie akcji dla wybranych alertów Możliwość importu plików MIB Przesyłanie alertów „as-is” do innych konsol firm trzecich Możliwość definiowania ról administratorów Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. Zdalne uruchamianie diagnostyki serwera. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| Certyfikaty | <ul style="list-style-type: none"> 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 |

| | |
|---------------------------------|--|
| | <p>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.</p> <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: <ul style="list-style-type: none"> 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 |

| | |
|--|---|
| | <p>dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.</p> <ul style="list-style-type: none"> o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. o Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaze 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. <ul style="list-style-type: none"> • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |
|--|---|

2. Dyski twarde – 8 sztuk

| | |
|----------------------|----------------------|
| Minimalne wymagania: | |
| Rodzaj urządzenia: | Dysk twardy Hot-Plug |
| Pojemność: | 2,4 TB |
| Rodzaj obudowy: | 2.5" w ramce 3.5" |
| Interfejs: | SAS 12Gb/s |
| Prędkość obrotowa: | 10000 obr/min |

3. Access Point – 8 sztuk

| Kategoria | Parametr | Wartość minimalna |
|----------------------------|--|-------------------------------|
| Specyfikacja bezprzewodowa | Pasmo częstotliwości | 2.4 GHz, 5 GHz |
| | Minimalna prędkość transmisji danych (2.4 GHz) | 500 Mbit/s |
| | Minimalna prędkość transmisji danych (5 GHz) | 1000 Mbit/s |
| | Standard Wi-Fi | IEEE 802.11ax (Wi-Fi 6) |
| | Obsługa MIMO | Tak |
| | Modulacja | 1024-QAM, 256-QAM |
| | Bluetooth | Tak |
| | Typ anteny | Wewnętrzna, omnidirectionalna |

| | | |
|----------------|------------------------------------|----------------------|
| | Minimalny zysk anteny | 5.5 dBi |
| Łączność | Porty Ethernet LAN (RJ-45) | 1 |
| | Prędkość transmisji Ethernet LAN | 10, 100, 1000 Mbit/s |
| | Obsługa PoE | Tak |
| | Zakres napięcia DC | 12 V |
| Bezpieczeństwo | Szyfrowanie/bezpieczeństwo | OWE, WPA2, WPA3 |
| Cechy fizyczne | Wymiary maksymalne | 170x170x40mm |
| | Waga maksymalna | 520g |
| | Maksymalny pobór prądu | 11W |
| | Minimalny zakres temperatury pracy | 0-40°C |

4. Dyski twarde do macierzy dyskowej – 20 sztuk

| | |
|-------------------------------|--|
| Minimalne wymagania: | |
| Pojemność | min. 20000 GB |
| Typ | HDD (magnetyczny) |
| Format | Format 3,5 cala |
| Interfejs | SATA III (6.0 Gb/s) |
| Pamięć cache | min. 256 MB |
| Prędkość obrotowa | 7200 obr./ min. |
| Prędkość odczytu (maksymalna) | do 268 MB/s |
| Technologia zapisu | CMR |
| Niezawodność MTBF | do 2 500 000 godzin |
| Zgodność | Systemy NAS zoptymalizowane pod kątem pracy w trybie RAID z nieograniczoną liczbą dysków |
| Współczynnik obciążenia | do 550 (TB/rok) |

5. UPS – 1 sztuka

| | |
|--|--|
| Parametr | Wartość minimalna |
| Technologia | Online, podwójna konwersja („True On-Line Double Conversion”) |
| Klasyfikacja | VFI-SS-111 (zgodnie z normą EN 62040-3) |
| Zakres mocy | 10 kVA / 15 kVA / 20 kVA – możliwość wyboru odpowiedniej mocy w ofercie |
| Konfiguracja fazowa | Wejście 3-fazowe / wyjście 3-fazowe (3:3) lub wejście 3-fazowe / wyjście jednofazowe (3:1) |
| Napięcie wejścia | 380 / 400 / 415 VAC (dla 3-faz) – zakres regulacji (-53% do +30%) |
| THDi (zniekształcenie prądu wejściowego) | < 3% |
| Współczynnik mocy wejściowej (PF) | ≥ 0,99 |

| | |
|--|--|
| Parametr | Wartość minimalna |
| Napięcie wyjścia | 380 / 400 / 415 VAC (dla 3-faz) lub 220 / 230 / 240 VAC (dla jednofaz) |
| Współczynnik mocy wyjściowej | 1,0 |
| Regulacja napięcia wyjściowego | ±1% statycznie, ±2% dynamicznie |
| Zniekształcenia napięcia wyjściowego (THD) | < 1% (obciążenie liniowe) / <3% (obciążenie nieliniowe) |
| Efektywność | > 96% (dla normalnego trybu pracy) |
| Komunikacja i monitoring | USB, inteligentny port, możliwość karty SNMP, EPO/REPO, LCD panel |
| Tryb ECO / bypass | Tryb ECO i automatyczny bypass, również tryb konserwacyjny (maintenance bypass) |
| Warunki środowiskowe | Temperatura pracy zalecana 15-25 °C dla dłuższej żywotności baterii; instalacja w pomieszczeniu czystym, wentylowanym. |

6. Zarządzalne urządzenia sieciowe z obsługą VLAN PoE – 8 sztuk

| Lp. | Minimalne wymagania Zamawiającego | |
|------|--|--|
| I. | CECHY ZARZĄDZANIA | |
| 1. | Typ przełącznika | Zarządzany |
| 2. | Przełącznik wielowarstwowy | L2/L3 |
| 3. | Obsługa jakości serwisu (QoS) | Tak |
| 4. | Zarządzany w chmurze | Tak |
| 5. | Zarządzanie przez stronę www | Tak |
| 6. | Inspekcja ARP | Tak |
| 7. | Konfigurowanie ustawień lokalizacji (CLI) | Tak |
| 8. | Obsługa MIB | Y |
| II. | OCHRONA | |
| 9. | Funkcje DHCP | DHCP relay, DHCP server, DHCPv6 client |
| 10. | Lista kontrolna dostępu (ACL) | Tak |
| 11. | Zasady Listy Kontroli Dostępu (ACL) | 1024 |
| 12. | IGMP snooping | Tak |
| 13. | Ochrona hasłem | Tak |
| 14. | obsługuje SSH/SSL | Tak |
| 15. | Filtrowanie adresów MAC | Tak |
| 16. | Szyfrowanie / bezpieczeństwo | HTTPS, SSH, SSL/TLS |
| III. | PORTY I INTERFEJSY | |
| 17. | Podstawowe przełączanie RJ-45 Liczba portów Ethernet | 48 |
| 18. | Podstawowe przełączania Ethernet RJ-45 porty typ | Gigabit Ethernet (10/100/1000) |
| 19. | Ilość slotów Modułu SFP+ | 4 |
| 20. | Liczba portów USB 2.0 | 1 |

| | | |
|-------|--|---|
| IV. | SIEĆ | |
| 21. | Standardy komunikacyjne | IEEE 802.1D, IEEE 802.1w, IEEE 802.1s, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad |
| 22. | Obsługa 10G | Tak |
| 23. | Dublowanie portów | Tak |
| 24. | Protokół drzewa rozpinającego | Tak |
| 25. | Blokowanie head-of-line (HOL) | Tak |
| 26. | Prędkość transferu danych przez Ethernet LAN | 10,100,1000 Mbit/s |
| 27. | Kontrola wzrostu natężenia ruchu | Tak |
| 28. | Automatyczne MDI/MDI-X | Tak |
| 29. | Podpora kontroli przepływu | Tak |
| 30. | Agregator połączenia | Tak |
| 31. | Obsługa sieci VLAN | Tak |
| 32. | Liczba VLANs | 4094 |
| V. | PRZESYŁANIE DANYCH | |
| 33. | Wielkość tabeli adresów | 16000 wejścia |
| 34. | Zgodny z Jumbo Frames | Tak |
| 35. | Rozszerzenie Jumbo Frames | 9000 |
| VI. | FUNKCJE MULTICAST | |
| 36. | Obsługa Multicast | Tak |
| VII. | PROTOKOŁY | |
| 37. | Protokoły zarządzające | SNMP |
| VIII. | KONSTRUKCJA | |
| 38. | Możliwości montowania w stelażu | Tak |
| 39. | Przycisk reset | Tak |
| 40. | Diody LED | Tak |
| IX. | WYDAJNOŚĆ | |
| 41. | Procesor wbudowany | Tak |
| 42. | Taktowanie procesora | 800 MHz |
| 43. | Pojemność pamięci wewnętrznej | 512 MB |
| 44. | Wielkość pamięci flash | 256 MB |
| 45. | Aktualizacje oprogramowania urządzenia | Tak |
| X. | MOC | |
| 46. | Zasilacz dołączony | Tak |
| XI. | WARUNKI PRACY | |
| 47. | Zakres temperatur (eksploatacja) | -5 - 50 °C |
| 48. | Zakres temperatur (przechowywanie) | -25 - 70 °C |
| 49. | Zakres wilgotności względnej | 10 - 90% |
| 50. | Dopuszczalna wilgotność względna | 10 - 90% |

7. Zarządzalne urządzenia sieciowe z obsługą VLAN – 2 sztuki

| | |
|---|--|
| Parametr | Wymaganie minimalne |
| Typ urządzenia | Przełącznik sieciowy klasy L3 (Layer 3 Stackable Managed Switch) |
| Porty miedziane | minimum 8 × 10GBase-T RJ-45 (10/100/1000/10 000 Mb/s) |
| Porty światłowodowe | minimum 8 × SFP+ (10 Gb/s) z obsługą transceiverów 1 Gb i 10 Gb |
| Stacking | obsługa fizycznego lub logicznego stackowania (min. 8 urządzeń) |
| Przepustowość (switching capacity) | min. 640 Gb/s |
| Przepustowość pakietowa (forwarding rate) | min. 476 Mpps |
| Bufor pamięci | min. 12 MB |
| Tablica MAC | min. 64 000 wpisów |
| Routing | L2/L3, obsługa protokołów statycznych i dynamicznych (RIP, OSPF, VRRP, PIM, ACL, DHCP snooping, QoS) |
| Bezpieczeństwo | ACL, 802.1X, DoS Protection, SSH, SNMPv3, RADIUS/TACACS+, Storm Control |
| Redundancja | obsługa zasilania redundantnego (PSU) i wentylatorów hot-swap |
| Zarządzanie | CLI/SSH/Telnet, GUI (HTTPS), SNMP v1/v2c/v3, RMON, NetFlow/sFlow |
| Zasilanie | 230 V AC |
| Montaż | Rack 19" z kompletem uchwytów i akcesoriów |
| Wymiary | max. 1U (wysokość) |
| Hałas / emisja | zgodność z normami EN55032 Class A, poziom hałasu ≤ 50 dB |
| Warunki pracy | temperatura 0–50 °C, wilgotność 10–90 % bez kondensacji |
| Transceivery (wkładki) | w zestawie minimum 4 szt. SFP+ 10 Gb (DAC lub SR) oraz 4 szt. SFP 1 Gb (SX/LX) |
| Gwarancja producenta | min. 3 lat lub dożywotnia z wymianą NBD (Next Business Day) |
| Wsparcie techniczne | dostęp do aktualizacji firmware i dokumentacji technicznej przez okres gwarancji |
| Kompatybilność | pełna zgodność z istniejącą infrastrukturą Ethernet 1/10 GbE oraz standardami IEEE 802.3 |

8. 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 klastry 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 łącz 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:
 - 10 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 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 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 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 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 dwuskładnikowego 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).
 - Obsługę 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 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

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

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

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

Logowanie

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

Testy wydajnościowe oraz funkcjonalne

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.

9. Tokeny sprzętowe – 40 sztuk

1. Wymagania funkcjonalne i techniczne (minimalne)

1. Standardy: FIDO U2F oraz FIDO2 (WebAuthn/CTAP) – urządzenie FIDO® Certified; możliwość użycia w trybie MFA oraz logowania bezhasłowego (tam gdzie wspierane).
2. Interfejs: USB 2.0 Type-A; praca bez baterii i bez sterowników (HID), kompatybilność z USB-C.
3. Obsługa systemowa i usług: co najmniej Windows 10/11, macOS, Linux; współpraca z popularnymi usługami wspierającymi FIDO (np. Google, Microsoft itp.).
4. Sygnalizacja działania: przycisk z diodą LED lub równoważny mechanizm aktywacji.
5. Parametry środowiskowe: temp. pracy co najmniej 0–70°C; przechowywanie co najmniej –20–70°C.
6. Bezpieczeństwo: klucze prywatne generowane i przechowywane wyłącznie w urządzeniu; brak możliwości odczytu/klonowania z zewnątrz.
7. Kompatybilność organizacyjna: możliwość rejestracji wielu kont/usług na jednym kluczu; brak konieczności instalacji dodatkowego oprogramowania klienckiego (poza ewentualnymi narzędziami administracyjnymi).

2. Wymagania gabarytowe (kompaktowy rozmiar – klasa „mini”)

Ze względu na konieczność pracy w gniazdach USB umieszczonych gęsto obok siebie (laptopy, stacje dokujące) oraz minimalizację ryzyka uszkodzeń mechanicznych, Zamawiający wymaga, aby klucz posiadał kompaktowe wymiary nieprzekraczające wartości poniżej. Wymagania wynikają z potrzeb użytkowych i ergonomii stanowisk pracy.

- Długość całkowita urządzenia (L) ≤ 25 mm.
- Szerokość zewnętrznej obudowy w najszerszym miejscu (W) ≤ 13 mm (nie mniejsza niż standard wtyku USB-A).
- Grubość (T) ≤ 2,0 mm (mierzona poza metalową osłoną wtyku, w najszerszym miejscu obudowy).

Uwaga: Powyższe progi są podyktowane ograniczeniami przestrzennymi oraz mają na celu zapewnienie ergonomii i bezpieczeństwa użytkowania. Zamawiający dopuszcza rozwiązania równoważne.

3. Dostawa i wsparcie

- Urządzenia fabrycznie nowe; gwarancja min. 24 miesiące;
- W zestawie skrócona instrukcja użytkownika w jęz. PL lub EN (online lub druk);
- Wsparcie producenta/dystrybutora w zakresie aktualizacji oprogramowania sprzętowego, jeżeli dotyczy.

4. Przedmiotowe środki dowodowe (składane z ofertą)

- Karta katalogowa producenta potwierdzająca zgodność z FIDO U2F i FIDO2 oraz wymiary (L×W×T), temperatury pracy i wagę;

- Odnośnik/ID do listy FIDO® Certified (lub równoważny dokument producenta) dla oferowanego modelu;

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

1. Architektura / budowa
 - 1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 50 Klientów jednocześnie.
 - 1.2. **Błąd! Nie można odnaleźć źródła odwołania.:**
 - 1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
 - 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
 - 1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
 - 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
 - 1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
 - 1.3. Konfiguracja Architektury:
 - 1.3.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
 - 1.3.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.
2. Wymagania systemowe
 - 2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).
 - 2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
 - 2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2
 - 2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.
 - 2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9.
 - 2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych bezpłatnym (np. Microsoft SQL Server Express Edition).
 - 2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
3. Interfejsy
 - 3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
 - 3.2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
 - 3.3. System zapewnia integrację z modelem LLM.
4. Funkcjonalności systemu zarządzania infrastrukturą IT

4.1. Funkcjonalność Klienta

4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.

4.2. Funkcjonalność konsoli administracyjnej.

4.2.1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.

4.2.2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.

4.2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

4.3. Funkcjonalność panelu pracownika

4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.

4.4. Zarządzanie licencjami

4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.

4.5. Wzorce aplikacji i pakietów

4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.

4.6. Zarządzanie podatnościami

4.6.1. System musi posiadać zdolności do bieżąco i automatycznego identyfikowania podatności w zainstalowanym oprogramowaniu.

4.6.2. Wykrywanie podatności musi być oparte o analizę wzorców zainstalowanego oprogramowania i porównanie ich z globalnymi bazami podatności, takimi jak CVE (Common Vulnerabilities and Exposures).

4.6.3. System powinien posiadać co najmniej dwa wskaźniki umożliwiające ocenę poziomu ryzyka i priorytetyzację zagrożeń.

4.6.4. System musi mieć możliwość ustawiania powiadomień o wykrytych podatnościach.

4.6.5. System musi mieć możliwość automatycznego tworzenia incydentów w przypadku integracji systemu z systemem eHelpDesk.

- 4.6.6. Powinna istnieć funkcja raportowania z możliwością filtrowania wg urządzenia, typu podatności lub poziomu krytyczności.
- 4.7. Inwentaryzacja sprzętu komputerowego i urządzeń.
- 4.7.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączone do komputerów oraz monitorować historię ich połączeń.
- 4.8. Inwentaryzacja urządzeń sieciowych.
- 4.8.1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
- 4.9. Inwentaryzacja sprzętu.
- 4.9.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
- 4.10. Ochrona danych (DLP)
- 4.10.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwoleńmi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami
- 4.10.2. Kontrola i ochrona urządzeń (KU)
- 4.10.2.1. Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń. (DEVICE)
- 4.10.2.2. Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzeń USB. (REMOVABLE DEVICE)
- 4.10.2.3. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www. (WEB)
- 4.10.2.4. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych. (WLAN)
- 4.10.2.5. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera. (WORKING TIME)
- 4.10.3. Ochrona danych w użyciu (DU)
- 4.10.3.1. Podjęcie działania w momencie uruchomienia określonego procesu. (PROCESS)
- 4.10.3.2. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka. (CLIPBOARD)
- 4.10.3.3. Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu. (PRINTSCREEN)
- 4.10.3.4. Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym. (SCREEN MONITORING)
- 4.10.4. Ochrona danych w ruchu (DR)
- 4.10.4.1. Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów. (E-MAIL)

- 4.10.4.2. Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą. (CLOUD STORAGE)
- 4.10.4.3. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach. (FILE MOVE COPY)
- 4.11. Szyfrowanie dysków wewnętrznych oraz zewnętrznych
 - 4.11.1. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS_AES_256 i AES_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/deszyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany.
- 4.12. Zdalna administracja komputerami
 - 4.12.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.
- 4.13. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
- 4.14. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
- 4.15. Zdalna instalacja
 - 4.15.1. System musi umożliwiać zdalną instalację pakietów MSI i plików .exe, korzystając z Windows Management Instrumentation (WMI) oraz usługi Klient bez dodatkowych poświadczeń, wykorzystując lokalne i sieciowe repozytoria. Powinien obsługiwać tworzenie repozytorium instalatorów z możliwością dodawania aplikacji, zarządzania wersjami oraz kategoryzacji. System musi również umożliwiać tworzenie grup instalacyjnych, definiowanie schematów instalacyjnych i automatyzację procesu instalacji na nowych urządzeniach. Powinien zawierać kiosk aplikacji umożliwiający użytkownikom samodzielną instalację aplikacji oraz rejestrować i raportować wszystkie procesy instalacji, umożliwiając również ich przerwanie.
- 4.16. Zarządzanie Poprawkami i Aktualizacjami
 - 4.16.1. System musi zapewniać ciągłe monitorowanie i identyfikację brakujących aktualizacji systemowych i komponentów infrastruktury IT, oferując funkcje rozpoznawania niezainstalowanych poprawek, ich pobierania, oraz klasyfikacji. Musi umożliwiać aktualizacje bez zakłócania pracy użytkowników, zarówno zbiorowo jak i indywidualnie, z opcją szybkiego przywrócenia poprzedniego stanu systemu poprzez odinstalowanie niechcianych poprawek. System powinien również umożliwiać pomijanie niechcianych poprawek i dostarczać szczegółowe raporty dotyczące stanu aktualizacji oraz urządzeń, które mogą wymagać restartu.
- 4.17. Zdalne Zarządzanie Zaporą (Firewall)
 - 4.17.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.
- 4.18. Automatyzacja

- 4.18.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.
- 4.19. Zarządzanie magazynem IT
- 4.19.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.
- 4.20. Repozytorium
- 4.20.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.
- 4.21. Kody kreskowe
- 4.21.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.
- 4.22. Wysyłanie wiadomości
- 4.22.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.
- 4.23. System musi posiadać możliwość eksportu / importu treści.
- 4.24. Monitorowanie drukarek sieciowych i wydruków
- 4.24.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
- 4.25. Monitorowanie stron www
- 4.25.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.
- 4.26. Monitorowanie serwerów WWW
- 4.26.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
- 4.27. Monitorowanie dziennika zdarzeń
- 4.27.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
- 4.28. System musi umożliwiać monitorowanie komunikatów Syslog.

4.29. Monitorowanie pracy komputerów

4.29.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.

4.30. Monitorowanie uprawnień ACL

4.30.1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.

4.31. Monitorowanie sensorów

4.31.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.

4.32. Repozytorium CMDB

4.32.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.

4.33. Worktime manager

4.33.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika.

4.34. Raportowanie i eksport danych

4.34.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.

4.35. System musi zapewnić interfejs API.

4.35.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.

4.36. Powiadomienia

4.36.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.

4.37. Bezpieczeństwo

4.37.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

5. Wsparcie i pomoc

5.1.1. Pomoc techniczna

5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

- 5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.
- 5.1.1.3. Czas trwania usługi SLA wynosi maksymalnie do 30.06.2026.

11. Licencja na oprogramowanie serwerowe I – 1 sztuka

Wymagane minimalne parametry

Oprogramowanie Windows Server 2025 Standard (licencja na 16 rdzeni procesora, wersja OEM) lub równoważne.

Opis równoważności dla systemu Windows Server 2025 Standard:

1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.
2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat.
4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2016 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server
5. Licencja na system operacyjny musi być bez ograniczeń czasowych.
6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.
7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
8. System operacyjny musi posiadać graficzny interfejs użytkownika.
9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
 - a. zarządzania użytkownikami,
 - b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
 - c. możliwości przydzielania praw dostępu do zasobów sieciowych,
 - d. instalacji zdalnej oprogramowania z pakietów msi,
 - e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11.
10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center.
12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
15. System operacyjny musi posiadać obsługę pamięci USB jako monitora kłaster
16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego kłaster
17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;

22. System operacyjny musi posiadać obsługę PowerShell 5.1,
23. System operacyjny musi posiadać obsługę certyfikatów w Active Directory
24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

12. Licencja na oprogramowanie serwerowe II – 1 sztuka

Wymagane minimalne parametry

Oprogramowanie Windows Server 2025 Standard (licencja na 16 rdzeni procesora, wersja CSP) lub równoważne.

Opis równoważności dla systemu Windows Server 2025 Standard:

1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.
2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat.
4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2016 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server
5. Licencja na system operacyjny musi być bez ograniczeń czasowych.
6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.
7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
8. System operacyjny musi posiadać graficzny interfejs użytkownika.
9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
 - a. zarządzania użytkownikami,
 - b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
 - c. możliwości przydzielania praw dostępu do zasobów sieciowych,
 - d. instalacji zdalnej oprogramowania z pakietów msi,
 - e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11.
10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center.
12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
15. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra
16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra

17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zaporę musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
22. System operacyjny musi posiadać obsługę PowerShell 5.1,
23. System operacyjny musi posiadać obsługę certyfikatów w Active Directory
24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

13. Licencje dostępowe – 8 kompletów

1. Licencje dostępowe na użytkownika (5 sztuk) – ilość 8 kompletów
 - Wymagana licencja typu Cal User OEM do systemu Windows Server 2025 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.
2. Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2025 na użytkownika:
 - Licencja dostępowa dla użytkownika umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2025 typu User Cal z wdrożoną rolą Active Directory

CZĘŚĆ II

1. Szkolenia 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 maksymalnie 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.

2. Szkolenie z cyberbezpieczeństwa dla pracowników IT/Sec – 1 sztuka

Szkolenie dla pracowników IT w zakresie cyberbezpieczeństwa

Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa:

Szkolenie z cyberbezpieczeństwa dla pracowników IT.

Indywidualne warsztaty online z zakresu cyberbezpieczeństwa skierowane do administratorów sieci teleinformatycznej, obejmujące co najmniej następujące obszary:

1. Wprowadzenie do cyberbezpieczeństwa:
 - Czym jest cyberbezpieczeństwo?
 - Dlaczego cyberbezpieczeństwo jest ważne?
 - Kluczowe zagadnienia związane z cyberbezpieczeństwem.
 - Przegląd statystyk i trendów w cyberbezpieczeństwie.
2. Typy zagrożeń w cyberprzestrzeni:
 - Malware (wirusy, trojany, robaki itp.)
 - Ataki typu phishing i spear phishing
 - Ataki DDoS
 - Ataki ransomware
 - Zagrożenia związane z sieciami społecznościowymi.
3. Zasady bezpieczeństwa i praktyki:
 - Zarządzanie hasłami i uwierzytelnianie wieloskładnikowe
 - Zasady bezpieczeństwa e-mail
 - Bezpieczeństwo w sieciach bezprzewodowych
 - Bezpieczne przeglądanie internetu
 - Backup i odzyskiwanie danych
4. Bezpieczeństwo systemów i sieci
 - Zasady bezpieczeństwa systemów operacyjnych
 - Bezpieczeństwo sieci i firewall
 - Wprowadzenie do VPN
 - Bezpieczeństwo urządzeń IoT
 - Bezpieczeństwo w chmurze
5. Reagowanie na incydenty i planowanie awaryjne
 - Jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem
 - Zasady reagowania na incydenty

- Planowanie awaryjne i kontynuacja działalności
 - Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione
6. Aktualne trendy i przyszłość cyberbezpieczeństwa
- Sztuczna inteligencja i machine learning w cyberbezpieczeństwie
 - Kryptografia i blockchain
 - Bezpieczeństwo danych w erze Big Data
 - Przyszłość cyberbezpieczeństwa: wyzwania i możliwości

Przewiduje się, że szkolenie potrwa łącznie maksimum 8 godzin roboczych, rozłożonych na co najmniej 2 dni. Każda sesja będzie trwała 4 godziny obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

3. Szkolenie AD/Wirtualizacja/Kopie zapasowe – 1 sztuka

1. Szkolenie z zakresu Active Directory (AD):

Inicjatywa szkoleniowa dedykowana Active Directory ma za zadanie zapewnić uczestnikom wszechstronne przygotowanie do efektywnego zarządzania oraz ochrony infrastruktury Active Directory, stanowiąc fundament dla bezpiecznego i zrównoważonego zarządzania tożsamościami i dostępami w sieciowych ekosystemach organizacyjnych. Program szkoleniowy został skonstruowany tak, aby objąć spektrum zagadnień, poczynając od elementarnych, aż po zaawansowane moduły:

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

2. Szkolenie z zakresu zabezpieczeń wirtualizacji:

Inicjatywa ta jest skoncentrowana na intensyfikacji świadomości oraz ekspansji umiejętności technicznych związanych z aspektami bezpieczeństwa operacyjnego w środowiskach wirtualizowanych. Program szkoleniowy został zaprojektowany tak, aby oferować kompendium wiedzy obejmujące kluczowe segmenty:

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

3. Szkolenie z zakresu bezpieczeństwa kopii zapasowych:

Inicjatywa szkoleniowa skoncentrowana na bezpieczeństwie kopii zapasowych kieruje się ku dogłębnemu zrozumieniu i praktycznej maestrii w zakresie kreowania oraz administracji bezpiecznymi mechanizmami backupu danych, akcentując na kluczowych komponentach:

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

Cel szkolenia:

Podstawowym zamierzeniem niniejszego kursu szkoleniowego jest dostarczenie uczestnikom kompleksowego zestawu wiedzy teoretycznej oraz praktycznych kompetencji, które są krytyczne dla

skutecznego administrowania i nadzorowania bezpieczeństwem infrastruktury technologicznej informacyjnej. Szczególny nacisk kładziony jest na głębokie zrozumienie i zarządzanie systemem Active Directory, ekosystemami wirtualizacji oraz złożonymi strategiami implementacji systemów kopii zapasowych. Celem tego szkolenia jest nie tylko przekroczenie granic czysto teoretycznego przekazu wiedzy, ale przede wszystkim rozwinięcie praktycznych umiejętności aplikacyjnych, które umożliwią uczestnikom efektywne zabezpieczanie wartościowych zasobów informatycznych przed rosnącą gamą zagrożeń cyfrowych oraz zagwarantowanie nieprzerwanej operacyjności systemów informatycznych.

Poprzez syntezę teoretycznych fundamentów z realnymi aplikacjami praktycznymi, program ma na celu wyekwipowanie uczestników w niezbędne narzędzia do identyfikacji, adekwatnej reakcji oraz neutralizacji potencjalnych zagrożeń bezpieczeństwa cyfrowego. Ponadto, kurs stawia za cel wdrożenie uczestników w głębinę najlepszych praktyk i standardów branżowych, które stanowią o kształcie profesjonalnej codziennej praktyki. Skupienie się na tych elementach ma kluczowe znaczenie dla kształtowania w uczestnikach umiejętności nie tylko reaktywnych, ale przede wszystkim proaktywnych w kontekście zarządzania ryzykiem i ochrony infrastruktury IT. W rezultacie, program szkoleniowy ma na celu przygotowanie adeptów do pełnienia roli bastionu w obronie przed zagrożeniami, promując jednocześnie kulturę bezpieczeństwa informacyjnego, która jest fundamentem dla zrównoważonego rozwoju i innowacyjności w przestrzeni technologicznej organizacji.

Przewiduje się, że szkolenie odbędzie się online oraz potrwa łącznie maksimum 15 godzin roboczych, rozłożonych na co najmniej 3 dni. Każda sesja będzie trwała 5 godziny obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

4. Szkolenia powiązane z testami socjotechnicznymi – 1 sztuka

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

3. Przeprowadzenie kampanii socjotechnicznej (wysłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej).
4. Wykonanie raportu z testu socjotechnicznego w języku polskim.
5. Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa, ukierunkowanego na omówienie wyników kampanii socjotechnicznej oraz co najmniej:
 - a. wprowadzenie do cyberbezpieczeństwa:
 - czym jest cyberbezpieczeństwo;
 - dlaczego cyberbezpieczeństwo jest ważne;
 - kluczowe zagrożenia 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.

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

5. Szkolenie specjalistyczne dla informatyków – 2 sztuki

Celem zamówienia jest przeprowadzenie szkolenia z zakresu podstawowej konfiguracji urządzenia UTM, który zostanie dostarczony w ramach projektu, dla pracowników technicznych. Szkolenie ma na celu umożliwić uczestnikom zdobycie praktycznych umiejętności w zakresie konfiguracji, zarządzania oraz monitorowania urządzeń UTM, co przyczyni się do zwiększenia bezpieczeństwa sieciowego w organizacji.

Opis techniczny szkolenia:

Szkolenie obejmuje następujące moduły:

1. Przygotowanie do konfiguracji - uczestnicy nauczą się jak połączyć się z urządzeniem UTM oraz jak korzystać z interfejsu webowego do zarządzania urządzeniem.
2. Konfiguracja interfejsów sieciowych - nauka konfiguracji interfejsów Ethernet i VLAN, ustawień IP, maski podsieci itp.
3. Tworzenie reguł zapory sieciowej - praktyczne ćwiczenia z tworzenia reguł kontrolujących ruch między interfejsami oraz wchodzący i wychodzący ruch sieciowy.
4. Konfiguracja VPN - instrukcje dotyczące ustawień VPN, w tym typów tuneli, uwierzytelniania i szyfrowania.

5. Monitorowanie i diagnostyka - przekazanie wiedzy na temat monitorowania urządzenia oraz technik diagnostycznych.
6. Aktualizacja oprogramowania - procedury aktualizacji oprogramowania urządzenia.
7. Zabezpieczenie dostępu - metody silnego uwierzytelniania i zapewnienie bezpieczeństwa dostępu do konfiguracji.
8. Tworzenie kopii zapasowych - nauka regularnego tworzenia i zarządzania kopiami zapasowymi.
9. Konsultacja dokumentacji i wsparcia technicznego - jak efektywnie korzystać z dostępnych zasobów wsparcia.
10. Monitoring bezpieczeństwa - konfiguracja systemów monitorujących bezpieczeństwo.

Zakres prac:

- Organizacja i przeprowadzenie serii warsztatów szkoleniowych.
- Dostarczenie materiałów szkoleniowych.
- Praktyczne ćwiczenia z użyciem urządzeń UTM.

Oczekiwane korzyści:

Uczestnicy szkolenia zdobędą umiejętności niezbędne do efektywnego i bezpiecznego zarządzania urządzeniami UTM, co zwiększy ogólną efektywność zarządzania infrastrukturą sieciową i poprawi poziom bezpieczeństwa IT w organizacji.

Przewiduje się, że szkolenie potrwa łącznie maksimum 8 godzin roboczych, rozłożonych na co najmniej 2 dni. Każda sesja będzie trwała 4 godziny obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

6. Wdrożenie SIEM – 1 sztuka

Dostawa oraz wdrożenie oprogramowania typu SIEM

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

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

Funkcjonalności systemu.

- Monitorowanie występujących zdarzeń (logów) w trybie ciągłym.
- Zbieranie zdarzeń z serwerów wirtualnych, fizycznych, Active Directory, przełączników oraz innego rodzaju urządzeń, które są oraz zostaną podłączone do infrastruktury zamawiającego.
- Agregacja oraz korelacja logów.
- Wykrywanie ataków typu brute force na różne usługi.
- Wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu.
- Analiza logów w oparciu o wbudowane reguły bezpieczeństwa.
- Konfiguracja oprogramowania do przechowywania logów z kluczowych zasobów przez okres 24 miesięcy zgodnie z rozporządzeniem KRI §21 pkt. 4 „Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.”
- Panel do wyszukiwania zdarzeń.

Wdrożenie systemu.

Wykonawca będzie odpowiedzialny za instalację i konfigurację oraz optymalizację środowiska systemu w infrastrukturze Zamawiającego oraz opiekę serwisową i wsparcie techniczne przez okres 30 dni.

Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:

- Przedstawienie architektury systemu.
- Omówienie procedur obsługi administracyjnej systemu;
- Omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń systemu;
- Przekazanie informacji na temat konfiguracji i zarządzania systemem;
- Instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną.

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

7. Opracowanie i wdrożenie dokumentacji SZBI – 1 sztuka

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

- Polityka Pracy Zdalnej musi określać zasady świadczenia pracy zdalnej, w tym wytyczne dotyczące zabezpieczenia aktywów oraz informacji przetwarzanych poza siedzibą organizacji, zgodnie z wymaganiami prawnymi i regulacyjnymi.
- Dokument powinien zawierać wytyczne dotyczące kontroli bezpieczeństwa, użycia narzędzi pracy oraz odpowiednich zabezpieczeń technicznych i organizacyjnych, zapewniając ochronę danych osobowych oraz tajemnic prawnie chronionych.

26. Polityka Bezpieczeństwa Zasobów Ludzkich

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

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

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

28. Oświadczenie o Przestrzeganiu Wymagań Dotyczących Bezpieczeństwa Informacji

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

29. Upoważnienie do Przetwarzania Informacji

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

30. Polityka Zarządzania Aktywami

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

31. Ewidencja Aktywów Podstawowych

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

32. Ewidencja Obszaru Przetwarzania Informacji

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

33. Polityka Kontroli Dostępu

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

34. Wymagania w Dostępie do Aktywów dla Personelu

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

35. Wymagania w Dostępie do Aktywów dla Podmiotów Zewnętrznych

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

36. Procedura Dostępu do Sieci i Usług Sieciowych

- Procedura Dostępu do Sieci i Usług Sieciowych musi określać zasady przyznawania dostępu do sieci i usług sieciowych wyłącznie uprawnionym użytkownikom, zgodnie z wymaganiami dotyczącymi identyfikacji, uwierzytelniania i autoryzacji.
- Dokument powinien zawierać wytyczne dotyczące sposobów dostępu, takich jak sieci przewodowe, bezprzewodowe, VPN, oraz połączenia zdalne, a także nadzór nad połączeniami przez Administratora Systemów Informatycznych.

37. Procedura Zarządzania Dostępem Użytkowników

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

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

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

39. Polityka Kryptografii

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

40. Polityka Bezpieczeństwa Fizycznego i Środowiskowego

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

41. Polityka Bezpiecznej Eksploatacji

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

42. Czynności Zabronione

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

43. Procedura Instalacji i Konfiguracji Systemów Informacyjnych

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

44. Procedura Konserwacji i Napraw Urządzeń Komputerowych

- Procedura Konserwacji i Napraw Urządzeń Komputerowych musi definiować zasady wykonywania konserwacji i napraw urządzeń komputerowych przez Administratora Systemów Informatycznych lub podmioty zewnętrzne, zgodnie z warunkami określonymi przez producenta.

- Dokument powinien zawierać wytyczne dotyczące nadzoru nad naprawami realizowanymi przez podmioty zewnętrzne oraz obowiązek usunięcia nośników danych lub informacji przed przekazaniem urzędów do serwisu zewnętrznego.

45. Procedura Obsługi Nośników Informacji

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

46. Procedura Użytkowania Systemów Informacyjnych

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

47. Procedura uruchamiania i Zatrzymania Komputera

- Procedura Uruchamiania i Zatrzymania Komputera musi definiować zasady prawidłowego uruchamiania komputera, w tym sprawdzenie połączeń, włączanie zasilania oraz proces uwierzytelniania użytkownika przy dostępie do systemu operacyjnego.
- Dokument powinien zawierać wytyczne dotyczące bezpiecznego zamykania systemu, odłączania urządzeń przenośnych oraz wyłączania komputera, zabraniając wyłączania poprzez bezpośrednie użycie przycisku zasilania poza sytuacjami awaryjnymi

48. Zasady Tworzenia i Postępowania z Hasłami

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

49. Polityka Zarządzania Bezpieczeństwem Sieci

- Polityka Zarządzania Bezpieczeństwem Sieci musi definiować zasady ochrony sieci organizacji, w tym zarządzanie urządzeniami sieciowymi, stosowanie zapór sieciowych, monitorowanie oraz uwierzytelnianie dostępu do sieci.

- Dokument powinien zawierać wytyczne dotyczące rozdzielania (segmentacji) sieci, bezpieczeństwa usług sieciowych oraz mechanizmów uwierzytelniania, szyfrowania i ograniczania dostępu do usług, zgodnie z umowami SLA i najlepszymi praktykami.

50. Polityka Przesyłania Informacji

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

51. Zasady korzystania z poczty Elektronicznej

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

52. Zasady Korzystania z Internetu

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

53. Umowa o Zachowaniu Poufności

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

54. Wymagania Związane z Bezpieczeństwem Systemów Informacji

- Wymagania Związane z Bezpieczeństwem Systemów Informacyjnych muszą obejmować zasady zabezpieczania systemów informacyjnych na każdym etapie ich cyklu życia, w tym identyfikację użytkowników, autoryzację, rejestrowanie działań oraz zarządzanie ryzykiem.

- Dokument powinien zawierać wytyczne dotyczące ochrony usług aplikacyjnych w sieciach publicznych, stosowania kryptografii oraz zabezpieczania transakcji, zapewniając poufność, integralność i dostępność przetwarzanych informacji.

55. Polityka bezpieczeństwa Informacji w Procesach Rozwoju i Wsparcia

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

56. Wymagania dotyczące Ochrony Danych Testowych

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

57. Polityka Bezpieczeństwa Informacji w Relacjach z Dostawcami

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

58. Zarządzanie Bezpieczeństwem Informacji przez Dostawcę

- Dokument Zarządzanie Bezpieczeństwem Informacji przez Dostawcę musi zawierać szczegółową ankietę oceniającą dostawcę pod kątem zgodności z wymaganiami dotyczącymi bezpieczeństwa informacji, w tym stosowania polityk ochrony danych osobowych, zarządzania ryzykiem oraz incydentami cyberbezpieczeństwa.
- Dokument powinien obejmować pytania dotyczące wdrożenia systemu zarządzania bezpieczeństwem informacji, zarządzania dostępem, szyfrowania oraz przestrzegania zasad „Privacy by design” i „Privacy by default”.

59. Procedura zakupu Oprogramowania i Urządzeń Komputerowych oraz Usług IT

- Procedura Zakupu Oprogramowania i Urządzeń Komputerowych oraz Usług IT musi definiować zasady inicjowania, realizacji i weryfikacji zakupów oprogramowania, urządzeń komputerowych oraz usług IT, w tym wymagania dotyczące bezpieczeństwa informacji zgodne z regulacjami prawnymi i wewnętrznymi.

- Dokument powinien zawierać wytyczne dotyczące sporządzania wniosku o zakup, który musi uwzględniać specyfikacje techniczne, planowane zabezpieczenia, potencjalnych dostawców oraz wymagania dotyczące bezpieczeństwa informacji i danych osobowych.
60. Polityka Zarządzania Incydentami, Zdarzeniami, Niezgodnościami i Słabościami
- Polityka Zarządzania Incydentami, Zdarzeniami, Niezgodnościami i Słabościami musi określać zasady postępowania w przypadku incydentów związanych z bezpieczeństwem informacji, w tym ich zgłaszania, oceny, podejmowania decyzji oraz działań zaradczych i korygujących.
 - Dokument powinien zawierać wytyczne dotyczące zgłaszania naruszeń danych osobowych do odpowiednich organów w terminie nie dłuższym niż 72 godziny oraz procedury reagowania na incydenty cyberbezpieczeństwa zgodnie z wymogami prawnymi.
61. Zgłoszenie Incydu, Zdarzenia, Niezgodności, Słabości
- Dokument "Zgłoszenie Incydu, 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 incydu, 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 Doskonałych
- Rejestr Incydentów, Zdarzeń, Niezgodności, Słabości, Działań Zaradczych, Korygujących i Doskonałych 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 doskonałych, 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 prądotwórczy – 1 sztuka

Poniżej przedstawiono szczegółowe minimalne wymagania dla agregatu prądotwórczego.

Agregat prądotwórczy ma być wykonany w obudowie zewnętrznej wyciszzonej, z blachy ocynkowanej ogniowo i malowanej proszkowo.

Solidna konstrukcja, która zapewnia łatwy dostęp do połączeń oraz części podczas przeglądów okresowych.

Dane wymiarowe:

Długość (L) mm- 2944

Szerokość (W) mm- 1150

Wysokość (H) mm- 1870

Waga (suchy) Kg- 2000

Pojemność zbiornika paliwa - min 280 L

Poziom hałasu

Poziom ciśnienia akustycznego z 7 m dB(A)- max 78

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

Agregat ma być wyposażony w nowoczesny silnik wysokoprężny zapewniający dobrą stabilizację częstotliwości i diagnostykę oraz w główne zabezpieczenie – wyłącznik kompaktowy.

W ramach dostawy zawarte mają być:

- a) dostawa agregatu w obudowie zewnętrznej o podanych parametrach na miejsce instalacji
- b) przeszkolenie obsługi pod względem prawidłowej eksploatacji
- c) pełna dokumentacja agregatu
- d) gwarancja 24 miesiące z limitem 1000 mth.
- e) producent agregatu posiadający certyfikaty ISO9001, ISO14001 ISO 45001

- f) dostawca musi posiadać autoryzację do obsługi serwisowej agregatu prądotwórczego (ASO – Autoryzowana Stacja Obsługi)

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.

Główne parametry agregatu .

Moc ciągła (PRP): min 140,00 kVA

Moc ciągła (PRP): min 112,00 kW

Moc awaryjna (E.P.): min 150,00 kVA

Moc awaryjna (E.P.): min 120,00 kW

Współczynnik mocy ($\cos\phi$): 0,8

Podłączenie: Trójfazowe, szeregowo-gwiazdowe

Napięcie trójfazowe: 400 V

Napięcie jednofazowe: 230 V

Częstotliwość: 50 Hz

Rodzaj paliwa: Diesel

Prądnica:

Moc PRP: 140,0 kVA

Moc EP: 150,0 kVA

Podłączenie: Trójfazowe, szeregowo-gwiazdowe

Stopień ochrony IP: 23

Dokładność: $1,00 \pm \%$

Silnik:

Liczba cylindrów: 6

Prędkość obrotowa: 1500 obr./min

Pojemność skokowa: max - 6,75 l

Doładowanie: Turbodoładowany

Napięcie standardowe: 12 V DC

Chłodzenie: Ciecz

Klasa dokładności: G3

ZABEZPIECZENIA Z ALARMEM

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

ZABEZPIECZENIA Z WYŁĄCZENIEM

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

INNE ZABEZPIECZENIA

- Wyłącznik awaryjny.
- Panel zabezpieczony zamykanymi drzwiami

ZUŻYCIE PALIWA

Zużycie 100% (P.P.): 33,40 l/h

Zużycie 100% (P.R.P.): 30,40 l/h

Zużycie przy 75% (P.R.P.): 23,10 l/h

Zużycie przy 50% (P.R.P.): 15,90 l/h

Czas pracy na pełnym zbiorniku przy 75% obciążenia – min 12 h

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

- Dla części I zamówienia:

CPV 72268000-1 usługi dostawy oprogramowania

CPV 48820000-2 serwery

CPV 48000000-8 pakiety oprogramowania i systemy informatyczne

CPV 72263000-6 Usługi wdrażania oprogramowania

- Dla części II zamówienia:

CPV 80550000-4 usługi szkolenia w dziedzinie bezpieczeństwa

- Dla części III zamówienia:

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 liczonych od dnia podpisania umowy w przedmiocie udzielenie zamówienia publicznego.

Szkolenia i Wdrożenia z części II będą realizowane w ciągu 180 dni, liczonych od dnia podpisania umowy w przedmiocie udzielenie zamówienia publicznego.

Dostawa Agregatu prądotwórczego z części III będzie realizowana w ciągu 45 dni, liczonych od dnia podpisania umowy w przedmiocie udzielenie zamówienia publicznego.

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

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

VII Warunki udziału w postępowaniu

1. O 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 gospodarczej lub 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 zrealizował należycie co najmniej dwa świadczenia w zakresie dostawy sprzętu komputerowego na kwotę co najmniej 250 000 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.
6. **Wykonawcy wspólnie ubiegają się o udzielenie zamówienia:**
 - a) Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia publicznego. W takim przypadku Wykonawcy występujący wspólnie są zobowiązani do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i zawarcia umowy w sprawie przedmiotowego zamówienia publicznego. Wszelka korespondencja będzie prowadzona przez Zamawiającego wyłącznie z pełnomocnikiem.
 - b) Warunek dotyczący uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej (o ile został sformułowany), o którym mowa w art. 112 ust. 2 pkt 2) ustawy Pzp, zostanie spełniony, jeżeli co najmniej jeden z Wykonawców wspólnie ubiegających się o udzielenie zamówienia posiada uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej i zrealizuje dostawy/usługi, do których realizacji te uprawnienia są wymagane.
 - c) W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać

na zdolnościach tych z Wykonawców, którzy wykonają dostawy/usługi, do realizacji których te zdolności są wymagane.

- d) W przypadku, o którym mowa Rozdziale VII SWZ (*o ile warunki udziału zostały sformułowane*), Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają odpowiednio do oferty oświadczenie, z którego wynika, które roboty budowlane wykonają poszczególni Wykonawcy.

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 2023 r. poz. 2048 oraz z 2024 r. poz. 1166) 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 2024 r. poz. 930),
 - 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. z 2021, poz. 1745),
 - 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. Zamawiający wymaga aby osoby odpowiedzialne za koordynację wykonania zamówienia po Stronie Wykonawcy (pracownik administracyjny/biurowy/stanowisko równoważne) zatrudniona była na podstawie stosunku pracy, o którym mowa w art. 22 § 1 Kodeksu pracy.
2. Obowiązek określony powyżej dotyczy również podwykonawców
3. 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.
4. Pozostałe osoby uczestniczące w wykonaniu zamówienia mogą współpracować z Wykonawcą na podstawie umów cywilnoprawnych.
5. 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: 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 - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów na rzecz, których dostawy zostały wykonane przed upływem terminu składania ofert, tj. co najmniej dwóch świadczeń w zakresie dostawy sprzętu komputerowego na kwotę co najmniej 250 000 złotych brutto wraz z dowodem należytego ich wykonania, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy, zgodnie ze wzorem stanowiącym załącznik nr 7 do SWZ.
 - Aktualne na dzień składania ofert oświadczenie, stanowiące wstępne potwierdzenie, że nie podlega wykluczeniu z postępowania oraz spełnia warunki udziału w postępowaniu, zgodnie ze wzorem stanowiącym załącznik nr 8 do SWZ.
 - Aktualne na dzień składania ofert oświadczenie sankcyjne, zgodnie ze wzorem stanowiącym załącznik nr 3 do SWZ.
 - Oświadczenie, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy o ochronie konkurencji i konsumentów – zgodnie ze wzorem stanowiącym załącznik nr 4 do SWZ.
 - 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 - 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 jeden z dwóch certyfikatów: Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE),
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, zgodnie ze wzorem stanowiącym załącznik nr 9 do SWZ 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 usługi lub dostawy, 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, o których mowa w rozdziale VIII niniejszej SWZ.
5. 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.
6. 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.
7. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia oświadczenia podmiotu udostępniającego zasoby – załącznik 9 do SWZ, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.

XIV Kryterium równoważności

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

XV Opis sposobu składania ofert w postępowaniu

1. Wykonawcy zobowiązani są do składania ofert, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej.
2. Wykonawca przygotowuje Formularz oferty, według wzoru stanowiącego załącznik nr 1 do SWZ.
3. Oferta powinna zawierać:
 - Formularz oferty, wg. wzoru załącznik nr 1 do SWZ.
 - 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. Sposób oraz termin składania ofert:
 - 4.1 Ofertę należy złożyć w terminie do dnia 12.12.2025r., do godziny 10⁰⁰ przez Platformę e- Zamówienia, strona dostępowa <https://ezamowienia.gov.pl/pl>
 - 4.2 Wykonawca składa ofertę za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania po zalogowaniu się na konto Wykonawcy. Po wybraniu przycisku „Złóż ofertę” system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola drag&drop („przeciągnij” i „upuść”) służące do dodawania plików.
 - 4.3 Wykonawca dodaje wybrany z dysku i uprzednio podpisany „Formularz oferty” w pierwszym polu („Wypełniony formularz oferty”). W kolejnym polu („Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”) wykonawca dodaje pozostałe pliki stanowiące ofertę lub składane wraz z ofertą.
 - 4.4 Jeżeli wraz z ofertą składane są dokumenty zawierające tajemnicę przedsiębiorstwa wykonawcy, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”. Zarówno załącznik stanowiący tajemnicę przedsiębiorstwa jak i uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa należy dodać w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.
 - 4.5 Formularz ofertowy podpisuje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Rekomendowanym wariantem podpisu wypełnionego Formularza oferty jest podpisanie go podpisem wewnętrznym. Jednakże w przypadku podpisania wypełnionego formularza innym wariantem tj. podpisem zewnętrznym Platforma również przyjmie taki formularz i przetworzy go prawidłowo w zakresie weryfikacji podpisu

pod warunkiem, że w przypadku tego wariantu podpisywania oddzielny plik z podpisem oferty zostanie załączony w sekcji „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”

- 4.6 Brak złożenia Formularza oferty zgodnie z powyższą instrukcją spowoduje odrzucenie oferty na podstawie art. 226 ust.1 pkt. 6 pzp, to jest Zamawiający uzna, że oferta nie została sporządzona lub przekazana w sposób zgodny z wymaganiami technicznymi oraz organizacyjnymi sporządzania lub przekazywania ofert przy użyciu środków komunikacji elektronicznej określonymi przez zamawiającego.
- 4.7 Pozostałe dokumenty wchodzące w skład oferty lub składane wraz z ofertą, które są zgodnie z ustawą Pzp lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym mogą być zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby opatrzone podpisem typu zewnętrznego lub wewnętrznego. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę” dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
- W przypadku przekazywania dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
- 4.8 System sprawdza, czy złożone pliki są podpisane i automatycznie je szyfruje, jednocześnie informując o tym wykonawcę. Potwierdzenie czasu przekazania i odbioru oferty znajduje się w Elektronicznym Potwierdzeniu Przesłania (EPP) i Elektronicznym Potwierdzeniu Odebrania (EPO). EPP i EPO dostępne są dla zalogowanego Wykonawcy w zakładce „Oferty/Wnioski”.
- 4.9 Oferta może być złożona tylko do upływu terminu składania ofert.
- 4.10 Wykonawca nie może wprowadzić zmian do złożonej oferty.
- 4.11 Wykonawca może przed upływem terminu składania ofert wycofać ofertę. Wykonawca wycofuje ofertę w zakładce „Oferty/wnioski” używając przycisku „Wycofaj ofertę”.
- 4.12 Maksymalny łączny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250 MB.

Zamawiający zastrzega, iż złożenie oferty w innej formie niż wskazana w SWZ i wynikająca z art. 63 ust.1 ustawy Pzp będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt 6 ustawy Pzp.

5. Termin otwarcia ofert:

Otwarcie ofert nastąpi w dniu 12.12.2025r. o godzinie 11:00 za pośrednictwem platformy e-Zamówienia.

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) | 90 |
| 2. | Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę | 10 |

- Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.
- W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.
- 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.

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

6. Sumaryczna liczba punktów zostanie obliczona według wzoru:

$$W = C + E$$

gdzie:

W – łączna liczba punktów przyznanych w poszczególnych kryteriach,

C – liczba punktów przyznanych w kryterium „Cena”,

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

Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku

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

8. W związku z zaistnieniem przesłanki o której mowa w art. 246 ust. 2 PZP możliwe było zastosowanie kryterium ceny jako kryterium o wadze przekraczającej 60%, ze względu na określenie w opisie przedmiotu

zamówienia wymagań jakościowych odnoszących się do co najmniej głównych elementów składających się na przedmiot zamówienia.

Do części II Zamówienia;

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

| Lp. | Nazwa kryterium | Waga (pkt) |
|-----|---|------------|
| 1. | Cena (całkowity koszt wykonania zamówienia) | 70 |
| 2. | Termin realizacji | 30 |

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 70% (maksymalnie do 70 pkt)
 - Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Oferty.
 - Punkty w kryterium „Cena” będą obliczane na podstawie wzoru:

$$C = CC_{\min} / CC_{\text{of}} \times 70$$

gdzie:

C – punkty przyznane Wykonawcy w ramach kryterium „Cena”

CC min – najniższa cena brutto spośród badanych ofert

CC of – cena brutto badanej ofert

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

5. Kryterium „Termin realizacji” stanowi maksymalnie do 30 pkt przy kryteriach:

- Do 180 dni – 0 pkt;
- Do 170 dni – 10 pkt;
- Do 160 dni – 20 pkt;
- Do 150 dni – 30 pkt.

6. Sumaryczna liczba punktów zostanie obliczona według wzoru:

$$W = C + E$$

gdzie:

W – łączna liczba punktów przyznanych w poszczególnych kryteriach,

C – liczba punktów przyznanych w kryterium „Cena”,

E – wartość punktowa kryterium „Termin realizacji”,

Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku

7. Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.
8. W związku z zaistnieniem przesłanki o której mowa w art. 246 ust. 2 PZP możliwe było zastosowanie kryterium ceny jako kryterium o wadze przekraczającej 60%, ze względu na określenie w opisie przedmiotu

zamówienia wymagań jakościowych odnoszących się do co najmniej głównych elementów składających się na przedmiot zamówienia.

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

1. 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”, Zamawiający informuje, że:

- 1) Administratorem Pani/Pana danych osobowych jest: Wójt Gminy Iwkowa, może Pani/Pan uzyskać informacje o przetwarzaniu Pani/Pana danych osobowych w Urzędzie Gminy w Iwkowej, z siedzibą 32-861 Iwkowa 468.
- 2) z Inspektorem ochrony danych osobowych wyznaczonym przez Administratora można kontaktować się pod adresem email: rodo@iwkowa.pl lub pod numerem telefonu 14 68-44-010, 14 68-44-020.
- 3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn. „Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd” w Gminie Iwkowa w ramach: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027”.
- 4) Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1 ustawy Pzp.
- 5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, 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; zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (tj. Dz.U z 2011 nr 14, poz. 67 z późn. zm.) teczki aktowe będą przechowywane w archiwum zakładowym przez okres 5 lat w przypadku dokumentacji zamówień publicznych oraz 10 lat w przypadku umów zawartych w wyniku postępowania w trybie zamówień publicznych.
- 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:
 - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących,
 - w przypadku, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 RODO wymagałoby niewspółmiernie dużego wysiłku, Zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu

sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego,

- w przypadku, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 RODO wymagałoby niewspółmiernie dużego wysiłku, Zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających w szczególności na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia publicznego,
- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (przy czym korzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników),
- 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 (przy czym prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
- wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 RODO, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego,
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, jeśli uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

9) nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,

- 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.
- 2. Jednocześnie Zamawiający przypomina o ciąży na Wykonawcy obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od Wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art. 14 ust. 5 RODO.
- 3. Skorzystanie przez osobę, której dane osobowe dotyczą, z uprawnienia do sprostowania lub uzupełnienia, o którym mowa w art. 16 RODO, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą Pzp.
- 4. W postępowaniu o udzielenie zamówienia zgłoszenie żądania ograniczenia przetwarzania, o którym mowa w art. 18 ust. 1 RODO, nie ogranicza przetwarzania danych osobowych do czasu zakończenia tego postępowania.

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 oraz informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami

1. Przedmiotowe postępowanie jest prowadzone przy użyciu środków komunikacji elektronicznej: za pośrednictwem Platformy e-Zamówienia: <https://ezamowienia.gov.pl/pl/>) oraz w uzasadnionych przypadkach, określonych w niniejszym pkt. 8 SWZ za pomocą poczty elektronicznej na adres e-mail: przetargi@iwkowa.pl (za wyjątkiem składania ofert i wycofania ofert).
2. Komunikacja w postępowaniu, z wyłączeniem składania ofert i wycofania ofert odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce „Formularze” („Formularze do komunikacji”). Za pośrednictwem „Formularzy do komunikacji” odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi.
Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk „dodaj załącznik”).
3. W przypadku załączników, które są zgodnie z ustawą Pzp lub rozporządzeniem ws. komunikacji elektronicznej (Dz. U z 2020r. poz. 2452) opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być opatrzone zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby, podpisem typu zewnętrznego lub wewnętrznego. W zależności od

rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).

4. Możliwość korzystania w postępowaniu z „Formularzy do komunikacji” w pełnym zakresie wymaga posiadania konta „Wykonawcy” na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Do korzystania z „Formularzy do komunikacji” służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie e- Zamówienia.
5. Wszystkie wysłane i odebrane w postępowaniu przez wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce „Komunikacja”.
6. Składanie ofert następuje za pośrednictwem modułu składania ofert i wniosków (MOW) Platformy e-Zamówienia.
7. Korzystanie z Platformy e-Zamówienia jest bezpłatne.
8. W szczególnie uzasadnionych przypadkach uniemożliwiających komunikację Wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia, w szczególności: awaria, brak działania Platformy e-Zamówienia, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres e-mail: przetargi@iwkowa.pl (za wyjątkiem składania ofert i wycofania ofert).
9. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto podmiotu „Wykonawca” na Platformie e- Zamówienia. Wykonawca posiadający konto na Platformie ma dostęp do formularzy: złożenia, wycofania oferty lub wniosku oraz do formularza do komunikacji.
Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej <https://ezamowienia.gov.pl> oraz informacje zamieszczone w zakładce „Centrum Pomocy”.
10. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie e-Zamówienia ani logowania.
11. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Instrukcji interaktywnej „oferty, wnioski i prace konkursowe” dostępnej pod adresem: <https://ezamowienia.gov.pl/komponent-edukacyjny/>
12. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji” wynosi

150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).

13. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia.
14. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu (22) 458 77 99 lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej (<https://ezamowienia.gov.pl>) w zakładce „Zgłoś problem”.
15. Sposób sporządzania oraz sposób przekazywania ofert, oświadczeń, podmiotowych i przedmiotowych środków dowodowych oraz innych informacji, oświadczeń lub dokumentów przekazywanych w postępowaniu o udzielenie zamówienia publicznego; wymagania techniczne dla dokumentów elektronicznych oraz wymagania techniczne i organizacyjne użycia środków komunikacji elektronicznej służące do odbioru dokumentów elektronicznych (oferta, oświadczenia, podmiotowe i przedmiotowe środki dowodowe oraz innych informacji, oświadczeń lub dokumentów przekazywanych w postępowaniu) zawiera niniejsza SWZ oraz Rozporządzenie ws. komunikacji elektronicznej (Dz. U z 2020r. poz. 2452).
16. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe odwzorowania) musi być zgodny z wymaganiami określonymi w rozporządzeniu ws. komunikacji elektronicznej (Dz. U z 2020r. poz. 2452).
17. Dokumenty elektroniczne, o których mowa w § 2 ust. 1 rozporządzenia ws. komunikacji elektronicznej (Dz. U z 2020r. poz. 2452), sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki.
18. Informacje, oświadczenia lub dokumenty, inne niż wymienione w § 2 ust. 1 rozporządzenia ws. komunikacji elektronicznej (Dz. U z 2020r. poz. 2452), przekazywane w postępowaniu sporządza się w postaci elektronicznej:
 - 1) w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (i przekazuje się jako załącznik),
lub
 - 2) jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków

komunikacji elektronicznej (np. w treści wiadomości e-mail lub w treści „Formularza do komunikacji”).

19. 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 oraz z 2021 r. poz. 1655) wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”.

20. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

21. Osoby uprawnione do komunikowania się z Wykonawcami:

Pan Piotr Dzięgiel – tel. (14) 6844010 wew. 15

22. Słowniczek pojęć:

- 1) Rozporządzenie ws. podmiotowych środków dowodowych (Dz. U z 2020 r. poz. 2415) – należy przez to rozumieć przepisy Rozporządzenia 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 r. poz. 2415)
- 2) Rozporządzenie ws. komunikacji elektronicznej (Dz. U. z 2020 r. poz. 2452) – należy przez to rozumieć przepisy Rozporządzenia 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 r. poz. 2452)
- 3) kwalifikowany podpis elektroniczny - oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego (art. 3 pkt 12 Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE)
- 4) podpis zaufany - podpis przynależny do profilu zaufanego na platformie ePUAP

Podpis zaufany zgodnie z art. 3 pkt 14a ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne (tekst jednolity Dz.U. 2021, poz. 2070) jest podpisem elektronicznym, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji, zawierającym dane identyfikujące osobę, ustalone na podstawie środka identyfikacji elektronicznej wydanego w nadzorowanym przez ministra właściwego do spraw informatyzacji systemie teleinformatycznym, który zapewnia obsługę publicznego systemu identyfikacji elektronicznej, w tym profilu zaufanego i profilu osobistego. Danymi identyfikującymi osobę w podpisie zaufanym są imię (imiona), nazwisko i numer PESEL. Ponadto podpis zaufany umożliwia identyfikację środka identyfikacji elektronicznej, przy użyciu którego został złożony i czasu jego złożenia.

- 5) podpis osobisty - podpis zdefiniowany w art. 2 ust. 1 pkt 9 ustawy z 6 sierpnia 2010 r. o dowodach osobistych (tekst jednolity Dz.U. 2021 po. 816 z późn. zm). Jest to zaawansowany podpis elektroniczny w rozumieniu art. 3 pkt 11 rozporządzenia eIDAS, weryfikowany za pomocą certyfikatu podpisu osobistego, czyli poświadczenia elektronicznego, które przyporządkowuje dane służące do walidacji podpisu osobistego do posiadacza dowodu osobistego, potwierdzające dane tego posiadacza. Certyfikaty podpisu elektronicznego stanowią warstwę elektroniczną dowodu osobistego i są wydawane przez ministra właściwego do spraw wewnętrznych.
- 6) **Oferta** - oświadczenie wykonawcy wyrażone w formularzu ofertowym, będące jednostronnym zobowiązaniem wykonawcy do wykonania oznaczonego świadczenia na rzecz zamawiającego. Brak załączenia formularza ofertowego oraz formularza cenowego będzie równoznaczne z brakiem złożenia oferty.
- 7) **Platforma e-Zamówienia** - elektroniczne zamówienia publiczne – platforma udostępniająca e-usługi w fazie pre-award procesu udzielania zamówienia publicznego, strona dostępowa Platformy: <https://ezamowienia.gov.pl/pl/>

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 poinformowany przez Zamawiającego o miejscu i terminie podpisania umowy.
4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią Załączniki Nr 2.1, 2.2, 2.3 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 zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo

b) zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o wyniku postępowania,

które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki.

10. Odwołanie zawiera:

1) imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);

- 2) nazwę i siedzibę zamawiającego, numer telefonu oraz adres poczty elektronicznej zamawiającego;
- 3) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub NIP odwołującego będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania albo posiada go nie mając takiego obowiązku;
- 4) numer w Krajowym Rejestrze Sądowym, a w przypadku jego braku - numer w innym właściwym rejestrze, ewidencji lub NIP odwołującego niebędącego osobą fizyczną, który nie ma obowiązku wpisu we właściwym rejestrze lub ewidencji, jeżeli jest on obowiązany do jego posiadania;
- 5) określenie przedmiotu zamówienia;
- 6) wskazanie numeru ogłoszenia w przypadku zamieszczenia w Biuletynie Zamówień Publicznych albo publikacji w Dzienniku Urzędowym Unii Europejskiej;
- 7) wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, lub wskazanie zaniechania przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy;
- 8) zwięzłe przedstawienie zarzutów;
- 9) żądanie co do sposobu rozstrzygnięcia odwołania;
- 10) wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności;
- 11) podpis odwołującego albo jego przedstawiciela lub przedstawicieli;
- 12) wykaz załączników.

Do odwołania dołącza się:

- 1) dowód uiszczenia wpisu od odwołania w wymaganej wysokości;
- 2) dowód przekazania odpowiednio odwołania albo jego kopii zamawiającemu;
- 3) dokument potwierdzający umocowanie do reprezentowania odwołującego.

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

ZAŁĄCZNIKI

- Załącznik nr 1 Formularz oferty
- Załącznik nr 2.1 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 Wykonawcy o braku przynależności do tej samej grupy kapitałowej
- 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
- Załącznik nr 9 Zobowiązanie podmiotu udostępniającego zasoby