SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego pn.: „Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny Samorząd” w Gminie Grodków 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””

Zatwierdził:
BURMISTRZ GRODKOWA
(-)
Miłosz Krok

Grodków, dnia 21 listopada 2024 r.

I. Zamawiający i postanowienia ogólne

Zamawiający:
Gmina Grodków
ul. Warszawska 29, 49-200 Grodków
tel. 77/ 4040300
e-mail: pm@grodkow.pl

Niniejszy dokument określa minimalne wymagania dla zamówienia z zakresu cyberbezpieczeństwa w ramach realizacji projektu „Cyberbezpieczny Samorząd" dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa".
Postępowanie prowadzone jest zgodnie z postanowieniami ustawy Prawo zamówień publicznych z dnia 11 września 2019 r. (Dz.U. z 2024 r. poz. 1320) oraz aktów wykonawczych wydanych na jej podstawie.
Niniejsze postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, w którym w odpowiedzi na ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani Wykonawcy, a następnie Zamawiający wybiera najkorzystniejszą ofertę bez przeprowadzenia negocjacji (art. 275 pkt 1 ustawy Pzp).

Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia:
https://platformazakupowa.pl/transakcja/1008070
Zamawiający w okresie 3 lat od dnia udzielenia zamówienia podstawowego, dotychczasowemu wykonawcy nie przewiduje udzielenia zamówienia polegającego na powtórzeniu podobnych usług.
Zamawiający nie przewiduje udzielenia zamówienia polegającego na zamówieniu dodatkowych dostaw.
Zamawiający dopuszcza składanie ofert częściowych na dowolnie wybrane części zamówienia spośród dwóch części.
Zamawiający nie dopuszcza składania ofert wariantowych.
Zamawiający nie przewiduje wymagań wskazanych w art. 96 ust. 2 pkt 2 ustawy Pzp.

Zamawiający nie przewiduje wymagań wskazanych w art. 94 ustawy Pzp.
Zamawiający nie przewiduje zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.
Zamawiający nie wymaga przeprowadzenia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy Pzp.
Zamawiający nie przewiduje rozliczenia między Zamawiającym a Wykonawcą w walutach obcych.
Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
Zamawiający nie wymaga obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań zgodnie z art. 60 i art. 121 ustawy Pzp.
Zamawiający nie przewiduje zawarcia umowy ramowej.
Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230 ustawy Pzp.
Zamawiający nie stawia wymogu lub możliwości złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93 ustawy Pzp.

Wykonawca jest związany ofertą nie dłużej **niż 30 dni** od dnia upływu terminu składania ofert. Pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert, zatem termin związania ofertą określa się: **od dnia 29.11.2024 r. do dnia 28.12.2024 r.**
W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa w zdaniu poprzedzającym, 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.

II. Definicje

Zamawiający dokonał opisu przedmiotu z wykorzystaniem następujących definicji:
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 przekracza wyrażoną w złotych równowartość kwoty określonej w art. 2 ust 1 pkt 1) ustawy prawo zamówień publicznych z dnia 11 września 2019 r. (Dz.U. z 2024 r. poz. 1320).

IV. Tajemnica przedsiębiorstwa

1. Zamawiający nie ujawnia informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (j.t. Dz. U. z 2022 r. poz. 1233 ze zm.), jeżeli Wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
2. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
   1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   2) cenach lub kosztach zawartych w ofertach.
3. Zastrzeżenie informacji może dotyczyć nie tylko oferty, ale i innych dokumentów czy informacji składanych przez wykonawcę w postępowaniu. Dla skuteczności dokonanego zastrzeżenia należy wypełnić następujące warunki:

a) Informacje stanowiące tajemnicę przedsiębiorstwa w całości lub części danego dokumentu powinny być złożone w oddzielnej części oferty (przykładowo w odrębnym folderze, dokumencie elektronicznym) i jednoznacznie oznaczone w nazwie pliku, dokumencie czy jego fragmencie.
b) Przykładowo w nazwie pliku oznaczenie: „Załącznik stanowiący tajemnicę przedsiębiorstwa" W przypadku treści dokumentu czy informacji oznaczenie fragmentu oznaczonego tajemnicą przedsiębiorstwa może zostać dokonane przykładowo poprzez oznaczenie kolorem, wskazanie punktów czy rozdziałów, dokumentu, w którym zawarte są informacje stanowiące tajemnicę przedsiębiorstwa.

4. Wykonawca ma obowiązek równocześnie z dokonanym zastrzeżeniem wykazać, że zastrzeżone informacje stanowią tajemnice przedsiębiorstwa. Wymagania w tym względzie normuje definicja tajemnicy przedsiębiorstwa: Ustawa o zwalczaniu nieuczciwej konkurencji w art. 11 ust. 2 wskazuje, że "przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności." Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust 5 Pzp oraz ust. 2 powyżej.

V. Opis przedmiotu zamówienia

Część 1

1. **Serwer – 1 sztuka.**

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz

	monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 256GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD)
Gniazda PCI	Min. dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT Dodatkowa karta SAS (4x mini SAS-HD, 12Gb/s, SAS, PCIe) Dodatkowa karta Dual Port (2x SFP+, 10Gb/s, SFP+, PCIe)
Dyski twarde	Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Wbudowane porty	4x USB, w tym min. 1 porty USB 3.0 2x port VGA (jeden na panelu przednim) Możliwość rozbudowy o Serial Port
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne, Hot-Plug
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium

Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: zdalny dostęp do graficznego interfejsu Web karty zarządzającej; zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; możliwość podmontowania zdalnych wirtualnych napędów; wirtualną konsolę z dostępem do myszy, klawiatury; wsparcie dla IPv6; wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; integracja z Active Directory; możliwość obsługi przez dwóch administratorów jednocześnie; wsparcie dla dynamic DNS; wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera

	możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej Przesyłanie danych telemetrycznych w czasie rzeczywistym Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych integracja z Active Directory Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram Szczegółowy opis wykrytych systemów oraz ich komponentów Możliwość eksportu raportu do CSV, HTML, XLS, PDF Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. Grupowanie urządzeń w oparciu o kryteria użytkownika Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach Szybki podgląd stanu środowiska Podsumowanie stanu dla każdego urządzenia Szczegółowy status urządzenia/elementu/komponentu Generowanie alertów przy zmianie stanu urządzenia. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń Integracja z service desk producenta dostarczonej platformy sprzętowej Możliwość przejęcia zdalnego pulpitu Możliwość podmontowania wirtualnego napędu Kreator umożliwiający dostosowanie akcji dla wybranych alertów Możliwość importu plików MIB Przesyłanie alertów „as-is” do innych konsol firm trzecich Możliwość definiowania ról administratorów Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów

	Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. Zdalne uruchamianie diagnostyki serwera. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.

	Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

2. **Serwer – 1 sztuka**

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych.

	Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 256GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD)
Gniazda PCI	Min. dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT Dodatkowa karta Dual Port (2x SFP+, 10Gb/s, SFP+, PCIe)
Dyski twarde	Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Wbudowane porty	4x USB, w tym min. 1 porty USB 3.0 2x port VGA (jeden na panelu przednim) Możliwość rozbudowy o Serial Port
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne, Hot-Plug
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: zdalny dostęp do graficznego interfejsu Web karty zarządzającej; zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; możliwość podmontowania zdalnych wirtualnych napędów; wirtualną konsolę z dostępem do myszy, klawiatury; wsparcie dla IPv6; wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; integracja z Active Directory; możliwość obsługi przez dwóch administratorów jednocześnie; wsparcie dla dynamic DNS; wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej Przesyłanie danych telemetrycznych w czasie rzeczywistym Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze Automatyczna rejestracja certyfikatów (ACE)

Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych integracja z Active Directory Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram Szczegółowy opis wykrytych systemów oraz ich komponentów Możliwość eksportu raportu do CSV, HTML, XLS, PDF Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. Grupowanie urządzeń w oparciu o kryteria użytkownika Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach Szybki podgląd stanu środowiska Podsumowanie stanu dla każdego urządzenia Szczegółowy status urządzenia/elementu/komponentu Generowanie alertów przy zmianie stanu urządzenia. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń Integracja z service desk producenta dostarczonej platformy sprzętowej Możliwość przejęcia zdalnego pulpitu Możliwość podmontowania wirtualnego napędu Kreator umożliwiający dostosowanie akcji dla wybranych alertów Możliwość importu plików MIB Przesyłanie alertów „as-is” do innych konsol firm trzecich Możliwość definiowania ról administratorów Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.

	Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. Zdalne uruchamianie diagnostyki serwera. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.

	Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.

	Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

3. **Serwer do wykonywania kopii zapasowych – 1 sztuka.**

Komponent	Minimalne wymagania
Obudowa i pojemność	Wysokość maksymalnie 1U do instalacji w szafie Rack. Co najmniej 9 slotów przeznaczonych na zestaw taśm.
Połączenie	Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów.
Napęd	Wyposażony w co najmniej 1 sztukę napędu SAS LTO8. W komplecie: • kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m • 10x taśma LTO8 WORM • Oznaczenia dla taśm LTO8, numery: 1-200 • Oznaczenia dla taśm LTO8 WORM, numery: 1-200 • 1 taśmy czyszczące
Gwarancja	5 lat gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma

	rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

4. **Network Attached Storage (NAS) - 1 sztuka**

Minimalne wymagania Zamawiającego	
Typ urządzenia	Serwer NAS
Obudowa	Rack 1U
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark 4 580 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 2 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 8 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą portu eSATA.
Porty zewnętrzne	Minimum:

	2 porty USB 3.2.1 1 port eSATA (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 2.0	Min. 1x 4-liniowe gniazdo x8 gen. 3
Wentylator obudowy	Min. 3 wentylatory (40 × 40 × 20 mm)
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	Maksymalny rozmiar pojedynczego wolumenu: 108 TB Minimalny liczba wewnętrznych wolumenów: 64 Minimalny liczba obiektów iSCSI Target: 128 Minimalny liczba jednostek iSCSI LUN: 256 Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	Minimalna liczba kont użytkowników: 2 048 Minimalna liczba grup użytkowników: 256 Minimalna liczba folderów współdzielonych: 512 Minimalna liczba jednoczesnych połączeń CIFS/AFP/NFS/FTP: 500* **Liczba jednoczesnych połączeń może zostać zwiększona do 2 000 po zainstalowaniu co najmniej 8 GB pamięci RAM.*
Uprawnienia	Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji
Wirtualizacja	Obsługa VMware vSphere with VAAI, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)

Obsługiwane przeglądarki	Google Chrome®, Firefox®, Microsoft Edge®, Safari® 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android™ 11.0 i nowsze) na tabletach
Oprogramowanie	Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Konserwacja	Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack

Gwarancja	3 lata na urządzenia główne 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack
Dodatkowa karta rozszerzeń	Dwa gniazda NVMe SSD M.2 Interfejs magistrali hosta: PCIe 3.0 x8 Interfejs pamięci masowej: PCIe NVMe Wysokość mocowania: Niskoprofilowe i o pełnej wysokości Obsługiwane obudowy: 22110 / 2280 Gwarancja: 5 lat

5. **Dyski twarde do NAS - 4 sztuki**

Minimalne wymagania:	
Pojemność	min. 8000 GB
Typ	HDD (magnetyczny)
Format	Format 3,5 cala
Interfejs	Serial ATA III
Pamięć cache	min. 256 MB
Prędkość obrotowa	7200 obr./ min.

6. Macierz dyskowa - 1 sztuka

Element konfiguracji/cecha/funkcjonalność	**Wymagania minimalne**
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U oraz umożliwiać montaż min. 12 dysków 3.5”
Przestrzeń dyskowa	Zainstalowane: 6x dysk SAS o pojemności min. 2.4TB, Hot-Plug 6x dysk NLSAS o pojemności min. 16TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej

	ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów iSCSI 25Gb (4 porty na kontroler),
Kable/wkładki	4x kabel DAC 25GbE SFP28-SFP28 min. 5m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.

	Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.

	Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w

	szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Warunki gwarancji	5 lat gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego,

	chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

7. UPS - 5 sztuk

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań
1	Moc pozorna	700 VA
2	Moc rzeczywista	360 W
3	Topologia (klasyfikacja IEC 62040-3)	Line-interactive
4	Liczba, typ gniazd wyjściowych	2 x FR

5	Typ gniazda wejściowego	1 x FR
6	Czas podtrzymania przy 50% obciążenia	6 minut
7	Tolerancja napięcia wejściowego	140-300V
8	Napięcie znamionowe wyjściowe	230 V
9	Zakres zmian napięcia wyjściowego (praca z baterii)	+/- 20%
10	Częstotliwość znamionowa wyjściowa	50/60 Hz
11	Zakres zmian częstotliwości wyjściowej (praca z baterii)	+/- 1 Hz
12	Układ automatycznej regulacji napięcia (AVR)	Tak
13	Kształt napięcia	modyfikowana sinusoida
14	Zimny start	Tak
15	Ochrona przed głębokim rozładowaniem	Tak
16	Interfejs komunikacyjny	• USB
17	Baterie wewnętrzne o pojemności	1x 7Ah/12V
18	Czas ładowania baterii do poziomy 90%	6 godz. do 90% pojemności użytkowej
19	Sygnały akustyczne	• Tryb bateryjny • Niski stan naładowania baterii • Przeciążenie • Wymiana baterii • Awaria
20	Sygnalizacja wizualna	dioda LED
21	Kolor	Czarny
22	Typ obudowy	Tower
23	Maksymalna szerokość	100 mm
24	Maksymalna wysokość	148 mm
25	Maksymalna głębokość	288 mm
26	Maksymalny ciężar	4,3 kg
27	Poziom hałasu	< 40 dBA dla pracy normalnej
28	Temperatura pracy	0 do 40 stopni C.
29	Znaki bezpieczeństwa	CE, TUV, raport CB
30	Bezpieczeństwo	IEC/EN 62040-1
31	Kompatybilność EMC	IEC/EN 62040-2
32	Gwarancja producenta 24 miesiące	Tak

8. UPS - 10 sztuk

Lp.	**Nazwa elementu, parametru lub cechy**	**Opis wymagań**
1	Moc pozorna	650 VA
2	Moc rzeczywista	400 W

3	Układ zaawansowanej ochrony przeciwprzepięciowej (ASR)	Tak
4	Czas przełączenia na baterię	5 ms
5	Liczba, typ gniazd wyj. z podtrzymaniem zasilania i ochroną przepięciową	3 x FR
6	Liczba, typ gniazd wyj. z ochroną przepięciową	1 x FR
7	Funkcja EcoControl	1 gniazdo sterowane EcoControl (automatyczna dezaktywacja nieczynnych urządzeń peryferyjnych)
8	Typ gniazda wejściowego	IEC320 C14 (10A)
9	Czas podtrzymania dla obciążenia 70%	5 min
10	Czas podtrzymania przy obciążeniu 50%	9 min
11	Napięcie znamionowe wejściowego	230 V
12	Tolerancja napięcia wejściowego	184 V – 264 V (regulacja 161 V – 284 V)
13	Częstotliwość znamionowa	50/60 Hz auto-selekcja
14	Tolerancja częstotliwości	46 – 70 Hz
15	Napięcie znamionowe wyjściowe	230 V (domyślnie), 220/240 V
16	Zakres zmian napięcia wyjściowego	+6/-10% napięcia nominalnego
17	Baterie wymieniane przez użytkownika	Tak
18	Baterie wewnętrzne o pojemności	1 x 7Ah 12V
19	Porty komunikacji	USB, HID
20	Ochrona linii danych	Tel., Fax, Modem, Internet i Ethernet
21	Ochrona przepięciowa	Tak (zgodnie z IEC 61643-1) 525 J
22	Panel sterowania diodowy	min. 2 diody LED
		• stan ostrzegawczy/awaria
		• stan przeciążenia na gniazdach z podtrzymaniem bateryjnym
23	Alarmy dźwiękowe	• awaria UPSa
		• przeciążenie UPSa
		• niski stan naładowania baterii
24	Przyciski	• Przycisk podświetlany ON/OFF LED załączania/ wyłączenia gniazd wyjściowych z podtrzymaniem bateryjnym
25	Kolor	Czarny
26	Typ obudowy	Uniwersalna Tower/Rack (możliwość instalacji pionowej, poziomej oraz w szafie Rack 19")
27	Wyposażenie standardowe	• kabel USB
		• oprogramowanie na CD

		• 1 x kabel zasilający zakończony wtykiem FR (PL)
		• instrukcja obsługi w języku polskim
28	Dołączone oprogramowanie	Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii kompatybilne z: Windows 7 / Vista/XP, Mac X OS, Linux
29	Maksymalna szerokość	81 mm
30	Maksymalna wysokość	263 mm
31	Maksymalna głębokość	235 mm
32	Maksymalny ciężar	3,6 kg
33	Cechy	Brak wentylatora, cicha praca, konstrukcja energooszczędna
34	Zimny start	Tak
35	Uruchomienie z baterii	Tak
36	Ochrona przed przeładowaniem	Tak
37	Gwarancja producenta 24 miesiące	Tak
38	Certyfikat CE	Tak

9. UPS – 1 sztuka

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań
1	Moc pozorna	5000 VA
2	Moc rzeczywista	4500 W
3	Topologia (klasyfikacja IEC 62040-3)	On-line z korekcją współczynnika mocy
4	Sprawność przy pracy normalnej (100% obc.)	>93,5%
5	Sprawność w trybie podwyższonej sprawności (100% obc.)	>98%
6	Współczynnik mocy	0,9
7	Czas przełączenia na baterię	0 ms
8	Możliwość pracy równoległej	Tak
9	Liczba, typ gniazd wyjściowych	Listwa zaciskowa, 8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza) po 4 x IEC C13, 2 x IEC C19 16A
10	Typ gniazda wejściowego	Listwa zaciskowa
11	Czas podtrzymania dla 100% obciążenia dla pf=0,9	3 min
12	Czas podtrzymania przy 50% obciążenia dla pf=0,9	11 min

13	Dodatkowe bateriie	Możliwość dodania do 12 dodatkowych modułow baterii w celu wydłużenia czasu podtrzymania do 242 minut dla 100% obciążenia przy pf=0,9
14	Napięcie znamionowe	200/208/220/230/240 V
15	Tolerancja napięci prostownika	176V – 276 V (100-276V przy 40% obciążenia)
16	Częstotliwość znamionowa	50/60 Hz autodetekcja
17	Tolerancja częstotliwości	40– 70 Hz
18	Kształt napięcia	Sinusoidalny
19	Napięcie znamionowe wyjściowe	230 V (domyślnie) / możliwość wyboru 200/208/220/240 V
20	Zakres zmian napięcia	+/-1% napięcia nominalnego
21	Częstotliwość wyjściowa	50/60 Hz +/-0,5%
22	Współczynnik szczytu	3:1
23	Dopuszczalny zakres współczynnika mocy obc. Liniowego	0,5 indukcyjny - 0,5 pojemnościowy
24	Baterie wymieniane przez użytkownika "na gorąco"	Tak
25	Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
26	Ochrona przed głębokim rozładowaniem	Tak
27	Okresowy automatyczny test baterii	Tak
28	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
29	Zdolność zwarciowa	90A
30	Możliwość uruchomienia bez napięcia w sieci	Tak
31	Baterie wewnętrzne o pojemności nie mniejszej niż	5Ah 12V, minimum 15 szt.
32	Czas ładowania baterii do poziomu 90%	< 1,5 godz. do 90% pojemności użytkowej
33	Interfejs komunikacyjny	• USB
		• RS232 DB-9 żeński (HID)
		• styki przekaźnikowe
		• miniport wyłącznik ON/OFF

		• SNMP/Ethernet
34	Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny,napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii).
		• Poziomy rząd przycisków sterowania
		• Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
		• Sygnalizator akustyczny
35	Sygnały akustyczne	• Awaria
		• Niski stan naładowania baterii
		• Przeciążenie
		• Serwis
36	Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie)
		• Przyciski funkcyjne (przewijanie w górę i w dół)
		• Przycisk Enter (potwierdzający)
		• Przycisk ON/OFF załączenia i wyłączenia
		• LED trybu zasilania z siec i(kolor zielony)
		• LED trybu baterii (kolor żółty)
		• LED usterki (kolor czerwony)
37	Kolor	Czarny RAL 9005
38	Typ obudowy	Uniwersalna Tower/Rack 3U
39	Wyposażenie standardowe	UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa
		1 x kabel szeregowy RS-232,
		1 x kabel komunikacyjny USB
		1 x CD Oprogramowanie
		2 x kable wyjściowe IEC 10A
		uchwyty kablowe
		1 x zestaw szyn montażowych 19’
		podstawki do montażu wieżowego
		1x karta sieciowa SNMP/Ethernet

40	Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych: - Windows: 7 / 8 / 2008 / Vista / 2003 / XP - Microsoft SCVMM 2012 - Linux: Debian GNU Linux: Lenny, SUSE/Novell: SLES 11, OpenSUSE 11.2, Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12 Ubuntu: 10.04 - VMWare: vCenter / ESXi 5.1 - Citrix XEN 6.0 Oprogramowanie musi posiadać funkcjonalność integracji (plug-in) z platformą wirtualizacyjną Vmware: vCenter Server.
41	Zgodność ze standardem Energy Star	Tak
42	Maksymalna szerokość	440 mm
43	Maksymalna wysokość	130 mm
44	Maksymalna głębokość	685 mm
45	Maksymalny ciężar	48 kg
46	Poziom hałasu w odl. 1m	do 45 dBA dla pracy normalnej
47	Znaki bezpieczeństwa	CE, C-Tick, UL
48	Gwarancja producenta	24 miesiące dla elektroniki oraz baterii

10. Oprogramowanie serwera - 1 sztuka

Wymagane minimalne parametry

Oprogramowanie Windows Server 2022 Standard (licencja na 16 rdzeni procesora, wersja OEM) lub równoważne.

Opis równoważności dla systemu Windows Server 2022 Standard:

System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.

System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.

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.
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
Licencja na system operacyjny musi być bez ograniczeń czasowych.
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.
Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
System operacyjny musi posiadać graficzny interfejs użytkownika.
System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
zarządzania użytkownikami,
zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
możliwości przydzielania praw dostępu do zasobów sieciowych,
instalacji zdalnej oprogramowania z pakietów msi,
definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11.
System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center.
System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.

Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra
System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra
System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
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;
System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
System operacyjny musi posiadać obsługa PowerShell 5.1,
System operacyjny musi posiadać obsługa certyfikatów w Active Directory
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).

11. Oprogramowanie serwera - 2 sztuki.

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

RÓWNOWAŻNOŚĆ:

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

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Datacenter. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:

1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,

b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
22. Możliwość wykorzystania standardu http/2.
23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
26. Mechanizmy logowania w oparciu o: a) login i hasło,
    a. karty z certyfikatami (smartcard),
    b. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
    a. określonych grup użytkowników,
    b. zastosowanej klasyfikacji danych,
    c. centralnych polityk dostępu w sieci,
    d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
33. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
        - bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,
    c. zdalna dystrybucja oprogramowania na stacje robocze,
    d. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        - Dystrybucję certyfikatów poprzez http,
        - Konsolidację CA dla wielu lasów domeny,
        - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f. szyfrowanie plików i folderów,
g. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
h. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
i. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
j. serwis udostępniania stron WWW,
k. wsparcie dla protokołu IP w wersji 6 (IPv6),
l. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
n. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
o. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover
z jednoczesnym zachowaniem pozostałej funkcjonalności.
p. mechanizmy wirtualizacji mające wsparcie dla:
- dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- obsługi 4-KB sektorów dysków,
- nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
- możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

q. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
r. wsparcie dla rozwiązania Kubernetes.
s. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta

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

t. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
u. mechanizmy deduplikacji i kompresji na wolumenach.
v. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
w. mechanizm konfiguracji połączenia VPN do platformy Azure.
x. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
y. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
z. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

12. Oprogramowanie przeciwdziałające wyciekowi danych – 62 sztuki.

Oprogramowanie na licencji wieczystej z dwu letnim wsparciem na minimum 62 stanowisk.

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera

zarządzającego z klientem odbywa się przy pomocy agenta.

7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.

10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.
15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
    a. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
    b. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
    a. logowanie oraz wylogowanie użytkownika,
    b. włączenie oraz wyłączenie stacji roboczej,
    c. blokada oraz odblokowanie stacji roboczej,
    d. przejście w stan bezczynności stacji roboczej.

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

31. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
32. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
    a. aplikacje, z której zostały utworzone,
    b. lokalizację,
    c. adres URL,
    d. format pliku,
    e. zawartość pliku.
33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
34. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
    a. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
    b. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach

    zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
    c. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
    d. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
    e. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
    f. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
    g. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
        I. Dropbox,
        II. Google Drive,
        III. SharePoint,
        IV. OneDrive Business,
        V. OneDrive Personal.
    h. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,

i. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
j. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,
k. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,

35. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
36. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
37. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
38. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
39. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e- mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
40. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
41. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
42. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
43. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.

44. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
45. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
    a. numery kart kredytowych,
    b. numer PESEL,
    c. numer polskiego dowodu osobistego,
    d. polski numer paszportu,
    e. wyrażenia regularne,
    f. określone ciągi znaków,
    g. numer IBAN.
46. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
47. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).
48. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
49. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e- mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy").
50. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
51. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
52. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM.
53. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
54. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:
    a. audyt i logowanie wiadomości e-mail,
    b. audyt i logowanie operacji na plikach,
    c. wprowadzanie polityk zabezpieczeń do wiadomości e-mail.

55. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).
56. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
57. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
    a. Bezpieczeństwo danych:
        - Przegląd informacji o incydentach bezpieczeństwa.
        - Przegląd danych przychodzących.
        - Przegląd danych wychodzących.
        - Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.
        - Podłączane/odłączane urządzenia przenośne.
    b. Produktywność:
        - Przegląd informacji na temat produktywności użytkowników.
        - Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
        - Trendy.
    c. Eksploatacja sprzętu:
        - Przegląd informacji na temat eksploatacji sprzętu komputerowego.
        - Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
        - Eksploatacja drukarek.
        - Eksploatacji sieci.

2. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
3. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
4. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt.:
    - plików przenoszonych na nośniki USB i inne urządzenia przenośne,
    - plików przesłanych za pomocą wiadomości e-mail,
    - plików przesłanych za pomocą poczty webowej,
    - plików przesłanych do Internetu,

- plików wysłanych za pomocą komunikatorów,
- plików przesłanych na dyski chmurowe,
- analiza sposobu korzystania z aplikacji,
- analiza korzystania z Internetu,
- analiza wykorzystania porali do poszukiwania pracy.

13. Oprogramowanie do wykonywania kopii zapasowych - 10 uniwersalnych licencji.

Lp.	Minimalne wymagania Zamawiającego
I. **Wymagania ogólne**	
1.	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
2.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
3.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
II. **Całkowite koszty posiadania**	
1.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
2.	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3.	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
4.	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
5.	Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

6.	Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
7.	Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
8.	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9.	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
10.	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
11.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
12.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
13.	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
14.	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
15.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
16.	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
III.	**Wymagania RPO**
1.	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
2.	Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3.	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru
4.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać

	użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
5.	Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
6.	Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
7.	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
8.	Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
9.	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
10.	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
11.	Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
12.	Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
13.	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
14.	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
15.	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
IV.	**Wymagania RTO**
1.	Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
2.	Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
3.	Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w

	hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
4.	Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
5.	Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
6.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
7.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
8.	Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
9.	Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
10.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
11.	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
12.	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
13.	Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
14.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
15.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
16.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
17.	Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

18.	Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
19.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
20.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
21.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
22.	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
V.	**Ograniczenie ryzyka**
1.	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
2.	Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
3.	Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
4.	Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
5.	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
VI.	**Środowiska fizyczne**
1.	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
2.	Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
3.	Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
4.	Rozwiązanie musi wspierać system operacyjny macOS

5.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
6.	Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
7.	Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
8.	Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
9.	Rozwiązanie musi wspierać backup podłączonych dysków USB
10.	Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
11.	Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
12.	Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
13.	Rozwiązanie musi wspierać kontrolę pasma sieciowego
14.	Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
15.	Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
16.	Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
17.	Rozwiązanie musi wspierać technologię BitLocker
18.	Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
19.	Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
20.	Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
21.	Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
22.	Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform

23.	Rozwiązanie musi wspierać szyfrowanie
24.	Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
25.	Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
26.	Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
27.	Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
VII. **Monitoring**	
1.	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
2.	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
3.	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
4.	System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
5.	System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
6.	System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
7.	System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
8.	System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
9.	System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
10.	System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
11.	System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
12.	System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
13.	System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta

14.	System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
15.	System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
16.	System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
17.	System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4
VIII. **Raportowanie**	
1.	System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
2.	System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
3.	System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
4.	System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
5.	System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
6.	System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
7.	System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
8.	System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
9.	System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
10.	System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
11.	System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
12.	System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta

13.	System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
14.	System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
15.	System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
16.	System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
17.	System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

Część 2

1. Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego.

Przedmiot zamówienia

Przedmiotem zamówienia jest specjalistyczna usługa odmiejscowienia serwera plików Zamawiającego oraz dodatkowym osprzętem (dalej: Urządzenia) w serwerowni Wykonawcy z uwzględnieniem montażu oraz konfiguracji krytycznych kopii zapasowych w okresie nie krótszym niż 12 miesięcy lecz nie dłuższym niż do dnia 30.06.2026 r.

Usługa obejmuje:

- udostępnienie niezbędnej przestrzeni, w tym RACK dla 1 dla Urządzenia o wysokości 1U, pozwalającej na prawidłowe wykonywanie krytycznych kopii zapasowych Zamawiającego, zgodnie z przyjętą polityką bezpieczeństwa, zwłaszcza w zakresie realizacji kopii zapasowych;
- zapewnienie redundantnego zasilania elektrycznego o określonej mocy, niezbędnej do prawidłowego działania Urządzeń, pozwalającego na zachowanie ciągłości działania w zakresie dystrybucji energii elektrycznej;
- zapewnienie redundantnego łącza internetowego, włączając w to co najmniej dwa niezależne przyłącza światłowodowe do serwerowni;
- zapewnienie gwarantowanego łącza internetowego z SLA o przepustowości symetrycznej co najmniej 500/500 Mbps, zapewniającego czas reakcji na awarie nie krótszy niż 2h oraz czas usunięcia awarii nie krótszy niż 8h;

- zapewnienie odpowiednich warunków temperaturowych i wilgotnościowych dla taśm magnetycznych przez cały czas trwania usługi;
- zapewnienie redundancji klimatyzacji w ilości co najmniej 4 niezależnie działających klimatyzatorów, z niezależnym i autonomicznym źródłem zasilania pozwalającym na co najmniej sześciogodzinną pracę klimatyzacji w przypadku awarii zasilania;
- zapewnienie ochrony przeciwpożarowej z systemem gaszenia gazem HFC 227ea oraz systemem oddymiania pomieszczenia, w którym zlokalizowane zostaną Urządzenia;
- zapewnienie zasilania awaryjnego złożonego z urządzeń typu UPS oraz agregat prądotwórczy, zapewniającego podtrzymanie zasilania przez okres nie krótszy niż 6 godzin;
- zapewnienie bezpieczeństwa fizycznego Urządzeń, w tym co najmniej zapewnienie elektronicznego systemu kontroli dostępu do Urządzeń, całodobowej ochrony obiektu, monitoringu wizyjnego obiektu z przechowywaniem nagrań z serwerowni przez co najmniej 14 dni;
- serwisowanie infrastruktury serwerowni Wykonawcy, a w przypadku awarii Urządzeń, demontaż i wysyłka Urządzeń na adres wskazany przez Zamawiającego w celu wykonania serwisu naprawczego lub naprawy pogwarancyjnej;
- zapewnienie bezpiecznego szyfrowanego połączenia pomiędzy urządzeniami wskazanymi przez Zamawiającego, a Urządzeniami zlokalizowanymi w serwerowni Wykonawcy z wykorzystaniem urządzeń Wykonawcy po stronie Wykonawcy usługi;
- możliwość rozbudowy infrastruktury w przyszłości;
- brak możliwości dostępu do szafy, w której zlokalizowane są kopie zapasowe, osób innych niż pracownicy i współpracownicy Zamawiającego;
- zapewnienie możliwości korzystania z dodatkowych lokalnych usług serwisowych w zakresie obsługi Urządzeń.

2. Wdrożenie systemów teleinformatycznych

Wdrożenie klastra serwerów

Krok 1: Planowanie i Przygotowanie

- Określenie wymagań dotyczących infrastruktury, w tym sprzętu, sieci i przechowywania.
- Wybranie serwerów, które zostaną użyte jako węzły klastra. Upewnij się, że są one zgodne z wymaganiami wybranego oprogramowania.

- Skonfigurowanie łącza sieciowego i przestrzeni dyskowej, aby zapewnić odpowiednią przepustowość i pojemność.
- Zainstalowanie systemu operacyjnego na każdym węźle klastra.

Krok 2: Instalacja roli oprogramowania do wirtualizacji

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

Krok 3: Konfiguracja klastra

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

Krok 4: Konfiguracja wysokiej dostępności klastra

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

Krok 5: Tworzenie i Zarządzanie Maszynami Wirtualnymi

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

Krok 6: Testowanie i Monitorowanie

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

3. Wdrożenie systemów teleinformatycznych

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

B. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.

C. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.

D. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.

E. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.

F. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.

G. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.

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

I. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając

utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.

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

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

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

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

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

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

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

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

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

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

4. Wirtualizacja serwerów

1. Sprawdzenie wymagań systemowych:

- Weryfikacja serwerów pod kątem minimalnych wymagań systemowych dla wirtualizatora.

Minimalne wymagania:

- Wymagania sprzętowe:
- Procesor: 64-bitowy procesor z obsługą wirtualizacji (Intel VT lub AMD-V).
- Pamięć RAM: Co najmniej 4 GB, chociaż zalecane są większe ilości, szczególnie jeśli planujesz uruchamiać wiele wirtualnych maszyn.
- Dysk twardy: Przestrzeń dyskowa wystarczająca do zainstalowania systemu operacyjnego i aplikacji, oraz dodatkowo miejsce na przechowywanie plików wirtualnych maszyn.
- Karta sieciowa: Karta sieciowa wspierająca TCP/IP, najlepiej z obsługą Gigabit Ethernet.

Wymagania systemowe:

- Wersja systemu operacyjnego: Hyper-V jest dostępny w wybranych edycjach systemu Windows Server, takich jak Windows Server Standard, Datacenter, Essentials, i innych.
- Aktualizacje: Zalecane jest regularne stosowanie aktualizacji systemu operacyjnego i aktualizacji zabezpieczeń dla bezpieczeństwa i wydajności.
- Wymagania dotyczące wirtualizacji:
- Włączone funkcje wirtualizacji w BIOS/UEFI komputera.
- Wsparcie dla Second Level Address Translation (SLAT), jeśli chcesz uzyskać pełną wydajność wirtualizacji w systemie Windows 8 lub nowszym.

Wymagania dodatkowe:

1. Jeśli planujesz tworzyć klastry HA, wymagane jest co najmniej dwa fizyczne serwery z odpowiednim sprzętem i siecią.
2. Posiadanie odpowiednich zasobów sprzętowych, takich jak procesory, pamięć RAM i przestrzeń dyskowa.
2. **Instalacja systemu operacyjnego**:

- Zainstalowanie na serwerach odpowiedniej wersji systemu operacyjnego umożliwiającego wirtualizację.

3. **Włączenie funkcji Hyper-V**:

- Włączenie funkcji wirtualizacji w BIOS/UEFI oraz instalacja i konfiguracja odpowiednich ról i funkcji do zarządzania wirtualizacją.

4. **Konfiguracja sieci**:

- Skonfigurowanie sieci wirtualnych oraz interfejsów sieciowych do zapewnienia komunikacji między wirtualnymi maszynami, a także z siecią lokalną i zewnętrzną.

5. **Przygotowanie pamięci masowej**:

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

6. **Konfiguracja klastra**:

- Utworzenie klastra wirtualizacji poprzez dodanie serwerów i skonfigurowanie ustawień klastra, w tym nazwy, adresu IP, oraz trybu zasilania.

7. **Konfiguracja magistrali klastra**:

- Umożliwienie komunikacji między serwerami poprzez konfigurację magistrali klastra oraz lokalizację Quorum w odrębnej lokalizacji SMB.

8. **Wdrożenie wirtualnych maszyn**:

- Instalacja i konfiguracja wirtualnych maszyn, w tym zapewnienie odpowiedniej konfiguracji dla migracji w przypadku awarii.

9. **Testowanie i monitorowanie**:

- Przeprowadzenie testów funkcji HA i migracji wirtualnych maszyn, monitorowanie wydajności i stabilności klastra oraz wirtualnych maszyn.

10. **Zarządzanie i utrzymanie**:

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

5. Wdrożenie systemów teleinformatycznych

Wdrożenie oprogramowania do wykonywania kopii zapasowych:

1: Planowanie i Przygotowanie

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

2: Instalacja i Konfiguracja

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

3: Konfiguracja Backupu

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

4: Konfiguracja Replikacji (opcjonalnie)

- Konfiguracje odpowiedniego zadania replikacji, określając maszyny wirtualne źródłowe i docelowe, harmonogramy i inne parametry.
- Weryfikacja dostępności docelowego środowiska na przyjęcie replikowanych maszyn wirtualnych.

5: Testowanie i Wdrażanie

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

6: Monitorowanie i Administracja

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

6. Utrzymanie systemów teleinformatycznych

Usługi stałego wsparcia technicznego (II linia wsparcia IT)

Przedmiotem zamówienia jest świadczenie usług stałej opieki informatycznej dla Zamawiającego, obejmujących w ilości nie mniejszej niż 120 godzin oraz w okresie nie krótszym niż 12 miesięcy lecz nie dłuższym niż do dnia 30.06.2026 r.:

- pomoc zdalna w rozwiązywaniu problemów z serwerami i oprogramowaniem serwerowym;
- monitorowanie dostępności serwerów i usług;
- reagowanie na problemy związane z dostępnością serwerów;
- zarządzanie zmianami i wersjami oprogramowania serwerowego;
- instalacja i konfiguracja nowego oprogramowania i sprzętu;
- zarządzanie patchami i aktualizacjami oprogramowania;
- backup i odzyskiwanie danych;
- monitorowanie wydajności systemów i aplikacji;
- diagnozowanie i rozwiązywanie problemów z wydajnością;
- zarządzanie konfiguracją systemów i aplikacji;
- automatyzacja rutynowych zadań operacyjnych;
- analiza i interpretacja logów systemowych i aplikacji;
- reagowanie na alerty bezpieczeństwa generowane przez SIEM;
- analiza trendów i przewidywanie przyszłych problemów;
- wdrażanie i zarządzanie kontenerami i usługami mikrousług;
- konfiguracja i zarządzanie sieciami wirtualnymi;
- zarządzanie certyfikatami SSL/TLS;
- wdrażanie zasad bezpieczeństwa i konfiguracji firewalli;
- audyt konfiguracji i zabezpieczeń systemów;
- przeprowadzanie testów penetracyjnych i ocen ryzyka;
- zarządzanie użytkownikami i uprawnieniami;
- zarządzanie bazami danych (backup, tuning, aktualizacje);
- zarządzanie środowiskami deweloperskimi, testowymi i produkcyjnymi;
- wsparcie dla procesów CI/CD (Continuous Integration/Continuous Deployment);
- doradztwo w zakresie architektury systemów i aplikacji;
- optymalizacja kosztów usług chmurowych;
- zarządzanie kluczami szyfrowania i dostępem do danych wrażliwych;
- planowanie i testowanie ciągłości działania (DR/BCP);
- zarządzanie incydentami bezpieczeństwa i reagowanie na nie;
- konsultacje w zakresie najlepszych praktyk DevOps i bezpieczeństwa IT;
- analiza przyczynowa (Root Cause Analysis) dla incydentów IT;
- zarządzanie dokumentacją techniczną i operacyjną;
- wsparcie przy migracjach systemów i aplikacji;

- ocena zgodności z wymaganiami regulacyjnymi i standardami branżowymi;
- szkolenia użytkowników i personelu technicznego w zakresie obsługi systemów;
- monitorowanie zagrożeń w cyberprzestrzeni i aktualizacja zabezpieczeń;
- zarządzanie konfiguracją sieci i urządzeń sieciowych;
- ocena skuteczności zaimplementowanych środków bezpieczeństwa;
- wsparcie dla procesów skalowania infrastruktury IT;
- analiza potrzeb biznesowych i doradztwo technologiczne;
- optymalizacja procesów biznesowych za pomocą technologii IT;
- przeglądy architektury systemów pod kątem najlepszych praktyk i zaleceń;
- wsparcie w zakresie integracji systemów i aplikacji;
- zarządzanie środowiskami wirtualnymi i chmurowymi;
- ocena wykorzystania zasobów IT i rekomendacje dotyczące optymalizacji;
- zarządzanie zmianą w infrastrukturze IT i procesach operacyjnych.

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

7. Wdrożenie systemów teleinformatycznych

Dostawa i wdrożenie oprogramowania do monitorowania zasobów IT:

Wymagania w zakresie oprogramowania:

- Automatyczne odkrywanie sieci.
- Monitorowanie wydajności i dostępności.
- Zaawansowane wizualizacje danych, w tym wykresy, mapy i wykresy słupkowe.
- Wbudowane narzędzia do przetwarzania i analizy danych.
- Możliwość monitorowania przez SNMP, JMX, IPMI, agenta Zabbix i inne.
- Szeroka gama integracji z zewnętrznymi systemami.
- Elastyczność w konfiguracji elementów monitorowanych.
- Wsparcie dla monitorowania aplikacji, serwerów, sieci i urządzeń.
- Możliwość definiowania scenariuszy monitorowania.
- Rozbudowane opcje powiadomień i alarmów.
- Wsparcie dla skryptów i automatyzacji zadań.
- Monitorowanie transakcji biznesowych i aplikacji webowych.
- Wbudowane rozwiązania do diagnostyki i rozwiązywania problemów.

- Możliwość tworzenia niestandardowych wskaźników monitorowania.
- Skalowalność i możliwość monitorowania tysięcy urządzeń.
- Wsparcie dla monitorowania w chmurze i środowiskach wirtualnych.
- Zaawansowane raportowanie i analizy trendów.
- Integracja z systemami ticketowymi.
- Możliwość tworzenia dashboardów i paneli.
- Wsparcie dla różnorodnych systemów operacyjnych.
- Elastyczne opcje autentykacji i kontroli dostępu.
- Szyfrowanie komunikacji.
- Możliwość monitorowania baz danych.
- Wsparcie dla wysokiej dostępności i redundancji.
- Automatyczne odkrywanie urządzeń w sieci.
- Monitorowanie wykorzystania zasobów.
- Możliwość śledzenia zmian konfiguracyjnych.
- Integracja z rozwiązaniami do zarządzania konfiguracją.
- Możliwość zbierania danych z różnych źródeł.
- Wsparcie dla monitorowania środowisk kontenerowych.
- Możliwość definiowania zależności między monitorowanymi elementami.
- Zaawansowane filtrowanie i wyszukiwanie danych.
- Możliwość monitorowania poprzez proxy.
- Wsparcie dla niestandardowych skryptów monitorujących.
- Automatyczne wykrywanie problemów i anomalii.
- Możliwość grupowania urządzeń i aplikacji.
- Wsparcie dla monitorowania sieciowych urządzeń peryferyjnych.
- Możliwość tworzenia template'ów monitorowania.
- Wsparcie dla różnych metod zbierania danych (polling, trapper, SNMP traps).
- Możliwość tworzenia hierarchii monitorowania.
- Wsparcie dla wielojęzyczności interfejsu użytkownika.
- Możliwość zarządzania poprzez interfejs webowy.
- Zaawansowane opcje logowania i audytu.
- Wsparcie dla monitorowania poprzez protokół HTTPS.
- Możliwość definiowania zdarzeń i akcji.
- Możliwość monitorowania szyfrowanych połączeń.
- Integracja z systemami zarządzania logami.
- Wsparcie dla SNMP v3.

- Możliwość definiowania i monitorowania SLA.
- Wsparcie dla rozproszonego monitoringu.

Wymagania w zakresie wdrożenia oprogramowania:

Krok 1: Planowanie i Przygotowanie

- Określenie wymagań dotyczących monitorowania, obejmujące zarówno liczbę urządzeń, które będą monitorowane, jak i typy parametrów, których monitorowanie jest kluczowe dla działania infrastruktury IT. Dodatkowo, konieczne jest sprecyzowanie oczekiwanych powiadomień w przypadku wykrycia nieprawidłowości lub awarii.
- Dokonanie wyboru odpowiedniej platformy do instalacji narzędzia monitorującego, uwzględniając różnice między systemem operacyjnym Linux a Windows. W tym procesie istotne jest także przypisanie odpowiednich zasobów sprzętowych i sieciowych, aby zapewnić odpowiednią wydajność i dostępność narzędzia.
- Pobranie najnowszej wersji wybranego narzędzia do monitorowania zasobów IT oraz dokładnie zapoznaj się z dokumentacją. Zapoznanie się z dokumentacją pozwoli na lepsze zrozumienie funkcjonalności narzędzia oraz prawidłową konfigurację i wykorzystanie jego możliwości w procesie monitorowania infrastruktury IT.

Krok 2: Instalacja i Konfiguracja serwera (procesu centralnego) narzędzia do monitorowania zasobów IT

- Przeprowadzenie instalacji serwera, który pełni rolę centralnego procesu narzędzia do monitorowania zasobów IT. Począwszy od wybranej platformy, postępujemy zgodnie z precyzyjnie określonymi instrukcjami instalacyjnymi, które są dostępne w dokumentacji danego rozwiązania.
- Konfiguracja centralnego procesu narzędzia. W ramach konfiguracji, należy zapewnić odpowiedni dostęp do bazy danych. Możesz użyć różne systemy zarządzania bazami danych, takie jak MySQL, PostgreSQL lub SQLite.
- Ustalenie parametrów monitorowania, które obejmują specyficzne aspekty środowiska IT podlegające monitorowaniu. Dodatkowo, konieczne jest skonfigurowanie powiadomień, aby zapewnić odpowiednie reakcje na wykryte nieprawidłowości czy awarie. Poprzez precyzyjne skonfigurowanie tych ustawień, można efektywnie zarządzać monitorowanymi zasobami IT oraz szybko reagować na wszelkie pojawiające się problemy.

Krok 3: Instalacja i Konfiguracja Agentów wybranego narzędzia na Monitorowanych Hostach

- Instalacja agentów na wszystkich urządzeniach, które podlegają monitorowaniu, obejmując serwery, routery, przełączniki oraz inne istotne elementy infrastruktury IT.
- Konfiguracja agentów, aby komunikowały się z wcześniej zainstalowanym i skonfigurowanym serwerem.
- Określenie parametrów komunikacji, takich jak adres serwera monitorującego oraz porty, aby umożliwić płynną wymianę danych pomiędzy agentami a serwerem.

Krok 4: Konfiguracja Monitorowanych Parametrów i Wykresów

- Konfiguracja elementów monitorowania, takich jak elementy, wykresy, triggery i akcje, aby monitorować ważne parametry systemowe i aplikacyjne. Umożliwi to kompleksowe śledzenie wybranych parametrów, takich jak obciążenie CPU, zużycie pamięci, dostępność usług, wydajność aplikacji.
- Dostosowanie progów alarmowych dla trigerów, w celu uzyskania optymalnych powiadomień o ewentualnych awariach lub nieprawidłowościach w działaniu systemu. Warto zadbać o precyzyjne ustalenie progów alarmowych, aby uniknąć fałszywych alarmów oraz zapewnić skuteczną ochronę środowiska IT.

Krok 5: Testowanie i Optymalizacja

- Weryfikacja skonfigurowanych monitorów i triggerów, aby upewnić się, że działają zgodnie z oczekiwaniami. Testowanie powinno obejmować różne scenariusze działania systemu, aby zweryfikować skuteczność monitorowania w różnych warunkach. Poprawne działanie monitorów i trigerów jest kluczowe dla zapewnienia szybkiej reakcji na ewentualne problemy.
- Optymalizacja konfiguracji narzędzia do monitorowania zasobów IT, w celu zapewnienia wydajności i skuteczności monitorowania, np. poprzez dostosowanie interwałów sprawdzania.

Krok 6: Monitorowanie i Administracja

- Regularne monitorowanie stanu urządzeń i aplikacji za pomocą interfejsu narzędzia do monitorowania zasobów IT pozwoli szybko identyfikować ewentualne zagrożenia lub nieprawidłowości w działaniu systemu, co umożliwia szybką reakcję i zapobieganie poważnym problemom.
- Reagowanie na alarmy i zdarzenia, które występują w środowisku monitorowanym.

W przypadku pojawiających się alarmów i zdarzeń, podejmować niezbędne działania naprawcze w celu przywrócenia normalnego funkcjonowania systemu.

- Regularne aktualizowanie oprogramowania do monitorowania zasobów IT, zapewni dostęp do najnowszych funkcji i poprawek bezpieczeństwa, co jest kluczowe dla utrzymania wysokiej jakości monitorowania oraz zapewnienia zgodności z aktualnymi standardami i wymaganiami branżowymi.

8. Wdrożenie SIEM

Zamawiający na potrzeby 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.

1. Funkcjonalności systemu.
    1. Monitorowanie występujących zdarzeń (logów) w trybie ciągłym.
    2. Zbieranie zdarzeń z serwerów wirtualnych, fizycznych, Active Directory, przełączników oraz innego rodzaju urządzeń, które są oraz zostaną podłączone do infrastruktury zamawiającego.
    3. Agregacja oraz korelacja logów.
    4. Wykrywanie ataków typu brute force na różne usługi.
    5. Wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu.
    6. Analiza logów w oparciu o wbudowane reguły bezpieczeństwa.
    7. 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.”
    8. Panel do wyszukiwania zdarzeń.

2. 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.

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

1. Przedstawienie architektury systemu.
2. Omówienie procedur obsługi administracyjnej systemu;
3. omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń systemu;
4. przekazanie informacji na temat konfiguracji i zarządzania systemem;
5. instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną.

9. Utrzymanie stałego wsparcia technicznego i organizacyjnego w zakresie utrzymania i doskonalenia wdrożonych standardów bezpieczeństwa

1. Cel zamówienia.

Celem zamówienia jest wzmocnienie mechanizmów bezpieczeństwa oraz poprawa zgodności operacyjnej systemów teleinformatycznych Zamawiającego z wymogami stawianymi przez ROZPORZĄDZENIE RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwłaszcza w zakresie monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, w oparciu o normy:

a. PN-ISO/IEC 27001 - w odniesieniu do formy systemu zarządzania bezpieczeństwem informacji;
b. PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
c. 2) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;
d. 3) PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

2. Zakres zamówienia.

Usługa będzie obejmować stałe doradztwo i wsparcie w ilości godzin nie mniejszej niż 60 godzin oraz w okresie nie krótszym niż 12 miesięcy lecz nie dłuższym niż do dnia 30.06.2026 r. w celu optymalizacji procesów zarządzania bezpieczeństwem informacji przez zespół co najmniej 2 certyfikowanych audytorów, pełniących rolę Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, posiadających łącznie co najmniej poniższe certyfikaty:

a. certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338) lub równoważny (dopuszcza się inne normy europejskie, które swoim zakresem obejmują normę polską), w zakresie certyfikacji osób;
b. certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku lub równoważny (dopuszcza się inne normy europejskie, które swoim zakresem obejmują normę polską), w zakresie certyfikacji osób.

Usługa obejmować będzie również:

a. zapewnienie aktualizacji regulacji wewnętrznych w zakresie zmieniającego się otoczenia;
b. kontrolę aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację;
c. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz sugerowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
d. podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
e. bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób, o których mowa w podpunkcie d;
f. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem zagadnień takich jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym
g. odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

g. wsparcie w zakresie aktualizacji technicznych i organizacyjnych środków ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez monitorowanie dostępu do informacji, działania zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
h. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
i. wsparcie merytoryczne w zakresie zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
j. weryfikację zapisów w umowach serwisowych podpisanych ze stronami trzecimi, gwarantujących odpowiedni poziom bezpieczeństwa informacji;
k. ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
l. wsparcie merytoryczne w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, w szczególności w obszarach: dbałości o aktualizację oprogramowania, minimalizowania ryzyka utraty informacji w wyniku awarii, ochrony przed błędami, utratą, nieuprawnioną modyfikacją, stosowania mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, zapewnienia bezpieczeństwa plików systemowych, redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, niezwłocznego podejmowania działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
m. w przypadku pojawienia się incydentów naruszenia bezpieczeństwa informacji, wsparcie w bezzwłocznym zgłaszaniu w określony i z góry ustalony sposób do właściwych organów, umożliwiającym szybkie podejmowanie działań korygujących.

10. Testy penetracyjne

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.

Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:

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

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

- przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
- przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;
- dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
- wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
- tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
- precyzyjna konfiguracja reguł przechwytywania wiadomości;
- możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;

- pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
- żądania i odpowiedzi dostępne w edytorze http;
- narzędzie do ręcznej edycji i ponownego wstawiania żądań;
- narzędzie do analizy statystycznej tokenów sesji;
- możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz powrót do zapisanego miejsca;
- biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;
- możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;
- skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
- możliwość analizy docelowej aplikacji internetowych.
- narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.

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

W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

1. Rekonesans.
    1. Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję w celu stworzenia potencjalnej bazy loginów i haseł.
    2. Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi).
    3. zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych.
    4. Sprawdzenie występowania w wyciekach znalezionych loginów.

2. Enumeracja zasobów.
    1. Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz z określeniem ich wersji) działających w ramach usług.
    2. Skanowanie publicznej infrastruktury.
    3. Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.
    4. Sprawdzenie udostępnionych w sieci wewnętrzej plików i folderów w szczególności pod kątem występowania danych wrażliwych.
    5. Analiza dostępnych wewnątrz sieci, usług, protokołów i urządzeń.
3. Eksploitacja.
    1. Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.
    2. Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) – po uzgodnieniu z Zamawiającym.
    3. Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).
4. Eskalacja uprawnień.
    1. Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.
    2. Rozpoznanie zasobów wewnętrznych, przechodzenie na inne środowiska dostępne ze skompromitowanych w pkt.3 zasobów (lateral movement).
5. Raport z testu penetracyjnego.

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

11. Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami

Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami:

1. Przygotowanie kampanii socjotechnicznej;
   a. wybór i zakup przez Wykonawcę domeny (łudząco podobnej do domeny Zamawiającego), która zostanie wykorzystana do kampanii socjotechnicznej;
   b. opracowanie bazy mailingowej pracowników objętych kampanią socjotechniczną oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłośliwy kod pozwalający na mierzenie efektów kampanii;
   c. wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);
   d. wsparcie w zakresie dodania domeny wybranej do przeprowadzenia kampanii socjotechnicznej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców).
2. Przygotowanie spreparowanych zasobów służących wyłudzaniu informacji:
   a. serwer strony www z bazą danych powiązany z domeną, która została zakupiona w celu przeprowadzenia kampanii socjotechnicznej;
   b. wykonanie kopii strony internetowej Zamawiającego i umieszczenie jej pod spreparowanym adresem;
   c. wygenerowanie niezbędnych certyfikatów SSL;
   d. przygotowanie spreparowanego aktywnego dokumentu PDF, wyposażonego w autorski, niezłośliwy skrypt, którego celem jest zebranie informacji o użytkownikach, którzy dokonali otwarcia pliku PDF i uruchomienia niezłośliwego skryptu (w prawdziwej kampanii byłoby to złośliwe oprogramowanie);

e. utworzenie nowej podstrony, na której umieszczony zostanie spreparowany plik PDF;
f. przygotowanie konta mailowego, którego celem jest podszycie się pod jedną z osób wtajemniczonych w prowadzone testy phishingowe;
g. przygotowanie treści wiadomości e-mail i wyposażenie jej w mechanizmy pozwalające na przeprowadzenie tzw. detekcji umiejscowienia (uzyskanie adresu IP potencjalnej „ofiary").

3. Przeprowadzenie kampanii socjotechnicznej (wysłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej).
4. Wykonanie raportu z testu socjotechnicznego w języku polskim.
5. Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa, ukierunkowanego na omówienie wyników kampanii socjotechnicznej oraz co najmniej:
   a. wprowadzenie do cyberbezpieczeństwa:
      - czym jest cyberbezpieczeństwo;
      - dlaczego cyberbezpieczeństwo jest ważne;
      - kluczowe zagadnienia związane z cyberbezpieczeństwem;
      - przegląd statystyk i trendów w cyberbezpieczeństwie.
   b. typy zagrożeń w cyberprzestrzeni:
      - malware (wirusy, trojany, robaki itp.);
      - ataki typu phishing i spear phishing;
      - ataki DDoS;
      - ataki ransomware;
      - zagrożenia związane z sieciami społecznościowymi.
   c. zasady bezpieczeństwa i praktyki:
      - zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
      - zasady bezpieczeństwa e-mail;
      - bezpieczeństwo w sieciach bezprzewodowych;
      - bezpieczne przeglądanie internetu;
      - backup i odzyskiwanie danych.
   d. reagowanie na incydenty i planowanie awaryjne:
      - jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
      - zasady reagowania na incydenty;
      - planowanie awaryjne i kontynuacja działalności;

- Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

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

12. Szkolenie z cyberbezpieczeństwa dla kadry administracyjnej

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.

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

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

13. Szkolenie z cyberbezpieczeństwa dla kadry informatycznej

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

Czas trwania szkolenia przewidziano na 8 godzin roboczych w podziale na 2 dni szkoleniowe po 4 godziny roboczych z uwzględnieniem 4 przerw po 15 minut. Po każdym dniu szkolenia będzie 30 minut na pytania i odpowiedzi uczestników.
Usługi szkoleniowe realizowane będą hybrydowo, częściowo w siedzibie Zamawiającego, częściowo przy pomocy zdalnego połączenia z systemami Zamawiającego.

14. Szkolenie z oprogramowania przeciwdziałającemu wyciekowi danych

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

- Podstawowe informacje
- Licencjonowanie
- Wspierane systemy operacyjne
- Wdrożenie oprogramowania przeciwdziałającego wyciekowi danych

- Omówienie instalatora oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie serwera oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie agentów oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie klientów oprogramowania przeciwdziałającego wyciekowi danych
- Uruchomienie modułu analitycznego
- Analiza wycieków danych
- Filtrowanie i raporty z analizy
- Uruchomienie modułu przeciwdziałającego wyciekowi danych
- Uruchomienie szyfrowania BitLockerem
- Konfiguracja dostępu do urządzeń i portów
- Interfejs webowy oprogramowania przeciwdziałającego wyciekowi danych
- Minimalne wymagania systemowe dla omawianego oprogramowania
- Instalacja oraz konfiguracja modułu webowego oprogramowania przeciwdziałającego wyciekowi danych
- Analiza zachowań
- Zarządzenie kategoriami produktywności
- Kontrola WWW i aplikacji
- Alerty, raporty i konserwacja
- Zaawansowane DLP dla oprogramowania przeciwdziałającego wyciekowi danych
- Reguły DLP – tryby polityk
- Reguły ogólne
- Reguły aplikacji
- Po co nam kategorie danych?
- Inteligentne wyszukiwanie danych osobowych
- Czym są tagi i do czego służą?
- Reguły tagowania dla aplikacji, stron oraz lokalizacji

15. Szkolenie wirtualizacja/kopie zapasowe

Szkolenie z zakresu zabezpieczeń wirtualizacji:

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

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

Szkolenie z zakresu bezpieczeństwa kopii zapasowych:
Inicjatywa szkoleniowa skoncentrowana na bezpieczeństwie kopii zapasowych kieruje się ku dogłębnemu zrozumieniu i praktycznej maestrii w zakresie kreowania oraz administracji bezpiecznymi mechanizmami backupu danych, akcentując na kluczowych komponentach:
- Fundamenty Backupu i Jego Znaczenie w Kontekście Bezpieczeństwa IT: Inauguracyjny moduł kursu dokonuje eksplikacji kluczowych pojęć i terminologii związanej z procesem tworzenia kopii zapasowych, podkreślając ich nieodzowną rolę w kompleksowej strategii bezpieczeństwa technologii informacyjnych oraz w zapewnieniu nieprzerwanej operacyjności korporacyjnych ekosystemów. Uczestnicy zdobywają perspektywę na istotę backupów jako niezbędnej linii obrony przed incydentami, które mogą zagrozić ciągłości działania organizacji.

- Dogłębna Analiza Typologii Kopii Zapasowych: Kurs prowadzi przez szczegółowe wyjaśnienie różnorodności form backupów – od pełnych, przez przyrostowe, aż po różnicowe – oferując równocześnie pragmatyczne wytyczne dotyczące ich efektywnego planowania, konfiguracji i implementacji. Omówienie to jest kluczowe dla zrozumienia optymalnych metod zarządzania cyklem życia danych oraz dla maksymalizacji efektywności procesów backupu.
- Implementacja Nowoczesnych Rozwiązań Backupowych: Ten segment szkolenia koncentruje się na adaptacji oraz wykorzystaniu zaawansowanych technologii i oprogramowania backupowego, włączając w to systemy lokalne oraz oparte na chmurze, techniki deduplikacji danych, mechanizmy kompresji oraz szyfrowania. Przedstawione zostają najnowsze narzędzia i metodologie, które umożliwiają zwiększenie efektywności i bezpieczeństwa procesów archiwizacji danych.
- Weryfikacja Efektywności Backupu i Strategii Odtwarzania: Kurs zawiera kompleksowe instrukcje dotyczące testowania efektywności tworzonych kopii zapasowych oraz procedur przywracania danych, z naciskiem na strategie prewencji i reagowania na kryzysy takie jak ataki ransomware. Uczestnicy uzyskują wiedzę na temat kluczowych praktyk i procedur testowych, które zapewniają gotowość na scenariusze awaryjne.
- Procedury i Strategie Odzyskiwania Danych po Awarii: Finalny moduł edukacyjny zagłębia się w omówienie metodyk i praktycznych wytycznych szybkiego odzyskiwania funkcjonalności systemów po wystąpieniu incydentów. Szczególna uwaga poświęcona jest skutecznym strategiom odzyskiwania danych, które są fundamentem dla minimalizacji czasu przestoju i optymalizacji procesu odbudowy po awarii.

16. Szkolenie z UTM

Celem zamówienia jest przeprowadzenie szkolenia z zakresu podstawowej konfiguracji urządzeń Fortigate dla pracowników technicznych. Szkolenie ma na celu umożliwić uczestnikom zdobycie praktycznych umiejętności w zakresie konfiguracji, zarządzania oraz monitorowania urządzeń Fortigate, 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 Fortigate 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 Fortigate.

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

17. Szkolenie SIEM

Przedmiotem zamówienia jest przeprowadzenie kompleksowego szkolenia z zakresu obsługi i zarządzania systemem Security Information and Event Management (SIEM). Celem szkolenia jest zapewnienie uczestnikom wiedzy i umiejętności niezbędnych do efektywnego monitorowania, wykrywania oraz reagowania na zagrożenia bezpieczeństwa w czasie rzeczywistym.

Szkolenie będzie obejmować następujące zagadnienia:

1. Wprowadzenie do systemów SIEM oraz ich roli w zapewnianiu bezpieczeństwa informacji.
2. Omówienie możliwości systemów SIEM, w tym analiza logów, wykrywanie intruzów, reagowanie na zagrożenia oraz integracja z innymi narzędziami bezpieczeństwa.
3. Praktyczne aspekty zbierania, agregowania, indeksowania i analizowania danych bezpieczeństwa, w celu identyfikacji włamań, zagrożeń oraz anomalii behawioralnych.
4. Zarządzanie podatnościami: metody identyfikacji słabości systemów i aplikacji, oraz techniki korelowania ich z aktualnymi bazami danych dotyczącymi podatności.
5. Ocena konfiguracji systemu i aplikacji zgodnie z najlepszymi praktykami i standardami, w tym analiza zgodności z regulacjami takimi jak RODO/GDPR, PCI DSS, NIST.
6. Reagowanie na incydenty: strategie i procedury tworzenia reguł alarmowych oraz zarządzanie reakcją na wykryte zagrożenia.
7. Przykłady zastosowania i najlepsze praktyki w wykorzystaniu systemów SIEM w różnych środowiskach, w tym w infrastrukturze chmurowej i w systemach kontenerowych.

Szkolenie ma na celu przygotowanie uczestników do samodzielnego zarządzania systemem SIEM, zrozumienia zasad ich działania oraz umiejętności konfiguracji i adaptacji systemu do specyficznych potrzeb organizacji. Uczestnicy nauczą się, jak efektywnie monitorować i analizować bezpieczeństwo w swoich systemach, identyfikować i reagować na zagrożenia, a także jak stosować najlepsze praktyki w celu zwiększenia ogólnego poziomu bezpieczeństwa informacji.

Czas trwania szkolenia przewidziano na 8 godzin roboczych w ciągu jednego dnia, z uwzględnieniem 4 przerw po 15 minut. Po dniu szkolenia będzie 30 minut na pytania i odpowiedzi uczestników.

18. Opracowanie i wdrożenie dokumentacji SZBI

Szkolenie i warsztaty uwzględniające konsultacje w zakresie doskonalenia, monitorowania i wdrożenia zmian w systemie zarządzania bezpieczeństwem informacji

Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkolenia i warsztatów z zakresu Systemu Zarządzania Bezpieczeństwem Informacji dla pracowników Zamawiającego, obejmujących co najmniej następujące obszary:

a. omówienie podstawowych zasad bezpieczeństwa informacji, wynikających z SZBI;

b. objaśnienie definicji powiązanych z systemem zarządzania bezpieczeństwem informacji;

c. konteksty i potrzeby stron Z uwzględnieniem wymagań prawnych i regulacyjnych;

d. zakres i polityka systemu zarządzania bezpieczeństwem informacji;

e. cel systemu zarządzania bezpieczeństwem informacji;

f. klasyfikacja informacji;

g. metodyka szacowania ryzyka w ramach systemu zarządzania bezpieczeństwem informacji;

h. metodyka szacowania szansę w ramach systemu zarządzania bezpieczeństwem informacji;

i. omówienie zasad i zabezpieczeń w ramach deklaracji stosowania;

j. nadzór nad udokumentowana informacja;

k. przeglądy Oraz doskonalenie systemu zarządzania bezpieczeństwem informacji;

l. metodyka ewidencjonowania aktywów informacyjnych;

m. zarządzanie dostępem użytkowników;

n. umówienie technik, standardów i oprogramowania wspomagającego kryptografię;

o. polityki bezpieczeństwa informacji;

p. budowanie procedur w ramach systemu zarządzania bezpieczeństwem informacji;

q. odpowiedzialność za naruszenie zasad SZBI;
r. zasady zgłaszania i reagowania na incydenty;
s. bezpieczeństwo informatyczne w miejscu pracy.

Szkolenia dla pracowników zostaną przeprowadzone w formie stacjonarnej lub online. Szkolenie zrealizowane będzie w dwóch grupach: pracownicy administracyjni i kadra kierownicza. Celem części warsztatowej jest opracowanie przykładowych wzorów polityk, procedur i ram systemu zarządzania bezpieczeństwem informacji:

a. Przewodnik SZBI;
b. Definicje SZBI;
c. Konteksty i potrzeby stron;
d. Zakres i Polityka SZBI;
e. Cele SZBI;
f. Szacowanie ryzyka z uwzględnieniem zabezpieczeń wynikających z Deklaracji stosowania SZBI;
g. Deklaracja stosowania SZBI;
h. Nadzór nad udokumentowaną informacją;
i. Protokół z przeglądu zarządzania;
j. Rejestr niezgodności;
k. Ramy ewidencji aktywów informacyjnych;
l. Zarządzanie dostępem użytkowników;
m. Klauzule umowne: odpowiedzialności stron, zakończenie zatrudnienia lub zmiana zakresu umowy, bezpieczne przesyłanie informacji, bezpieczeństwo usług sieciowych, zapisy związane z poufnością informacji, wymagania odnoszące się do ryzyk;
n. Ogólne techniki, standardy kryptograficzne;
o. Ogólne standardy bezpieczeństwa informacji;
p. Ramy rejestru incydentów;
q. Procedury i polityki bezpieczeństwa informacji: Procedury szyfrowania transmisji danych w pracy zdalnej, Polityka pracy zdalnej i stosowania urządzeń mobilnych, Procedury weryfikacji kandydatów do pracy, Procedury postępowań dyscyplinarnych, Ewidencja aktywów informacyjnych, Polityka zarządzania aktywami informacyjnymi, Polityka klasyfikacji informacji, Procedury oznaczania informacji zgodnie z klasyfikacją, Procedury postępowania z aktywami informacyjnymi, Procedury zarządzania nośnikami informacji, Polityka kontroli dostępu, Procedury

nadawania i odbierania uprawnień, Zarządzanie dostępem użytkowników, Polityka haseł, Procedury bezpiecznego logowania, Polityka stosowania zabezpieczeń kryptograficznych, Procedury pracy w obszarach bezpiecznych, Procedury konserwacji sprzętu, Procedury przekazywania sprzętu, Procedury zarządzania sprzętem komputerowym, Polityka czystego biurka i czystego ekranu, Polityka zarządzania zmianą, Procedury monitorowania i wykorzystania zasobów, Procedury separacji środowisk pracy, Procedury ochrony przed szkodliwym oprogramowaniem, Polityka kopii zapasowych, Procedury tworzenia kopii zapasowych, Procedury rejestrowania zdarzeń i monitorowania, Procedury nadzoru nad instalacją oprogramowania, Procedury instalowania oprogramowania, Procedury zabezpieczenia audytu systemów informacyjnych, Polityka monitorowania sieci w trybie ciągłym, Polityka przesyłania informacji, Procedury przesyłania informacji, Polityka pozyskiwania, rozwoju i utrzymania systemów, Procedury przeglądu i kontroli zmian w systemach, Polityka bezpieczeństwa informacji w relacjach z dostawcami, Procedury zarządzania incydentem, Polityka ciągłości działania, Procedury zachowania ciągłości działania, Procedury zachowania zgodności, Procedury przeglądu bezpieczeństwa informacji;

r. Przegląd polityk bezpieczeństwa informacji (Audity wewnętrzne): Program auditów, Raport z auditu wewnętrznego.

Szkolenie oraz wzory polityk, procedur i ram systemu zarządzania bezpieczeństwem informacji powinny – zgodnie z §20 ust. 2 pkt 14 KRI - odnosić się do SZBI wdrożonego zgodnie z Polskimi Normami PN-ISO/IEC 27001 - w odniesieniu do SZBI, PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

19. Aktualizacja polityk bezpieczeństwa informacji

Polityka kopii zapasowych:

1. Ocena wymagań biznesowych i technologicznych:
   - Zrozumienie potrzeb firmy w zakresie kopii zapasowych.
   - Określenie kluczowych aplikacji, danych i systemów, które wymagają zabezpieczenia.

- Ustalenie priorytetów dotyczących przywracania danych.

2. Określenie zasobów do zabezpieczenia:
   - Zidentyfikowanie wszystkich systemów, danych i aplikacji, które należy uwzględnić w polityce kopii zapasowych.
3. Wybór odpowiednich narzędzi i technologii:
   - Przegląd dostępnych rozwiązań do kopii zapasowych, w tym oprogramowania i sprzętu.
   - Wybór narzędzi odpowiadających potrzebom i budżetowi firmy.
4. Ustalenie harmonogramu kopii zapasowych:
   - Określenie częstotliwości kopii zapasowych (codziennie, co tydzień, co miesiąc).
   - Planowanie godzin kopii zapasowych, aby minimalizować wpływ na działanie firmy.
5. Określenie retencji danych:
   - Zdefiniowanie, jak długo należy przechowywać kopie zapasowe.
   - Ustalenie, czy istnieją specjalne wymogi prawne dotyczące przechowywania danych.
6. Wybór lokalizacji kopii zapasowych:
   - Decyzja, czy kopie zapasowe powinny być przechowywane lokalnie, w chmurze lub na zewnętrznych nośnikach.
   - Warto również rozważyć zapewnienie kopii zapasowych w różnych lokalizacjach dla lepszej odporności na awarie.
7. Testowanie i weryfikacja polityki kopii zapasowych:
   - Regularne testowanie procesów przywracania danych, aby upewnić się, że są one skuteczne.
   - Weryfikacja, czy kopie zapasowe są integralne i możliwe do przywrócenia.
8. Zapewnienie dokumentacji:
   - Stworzenie dokumentacji opisującej politykę kopii zapasowych, wraz z procedurami przywracania danych.
   - Szkolenie personelu odpowiedzialnego za zarządzanie kopiami zapasowymi.
9. Monitorowanie i utrzymanie:
   - Regularne monitorowanie procesów kopii zapasowych w celu wykrywania ewentualnych problemów.
   - Aktualizacja polityki kopii zapasowych w miarę zmian w środowisku IT firmy.
10. Zarządzanie incydentami:

- Przygotowanie planu działania w przypadku awarii systemu lub utraty danych.
- Szybka reakcja na incydenty i przywracanie usług w możliwie najkrótszym czasie.

20. Aktualizacja polityk bezpieczeństwa informacji

Cel Usługi:

Podstawowym celem niniejszej usługi jest skonstruowanie polityki ciągłości działania dla systemów informatycznych oraz infrastruktury telekomunikacyjnej Zamawiającego. Taka polityka aspiruje do gwarantowania bezusterkowego dostępu do esencjonalnych usług oraz danych w przypadku wystąpienia wszelakich awarii, kataklizmów bądź innych nieoczekiwanych wydarzeń, co ma za zadanie zredukować potencjalne ryzyko przestojów i asocjowanych z nimi strat.

Zakres Usługi:

1. Analiza Stanu Istniejącego i Identyfikacja Wymagań:

- Egzekucja wnikliwej analizy aktualnego stanu infrastruktury ICT oraz przegląd dotychczasowych strategii z zakresu ciągłości działania, mających na celu zdiagnozowanie potencjalnych luk i niedoskonałości.
- Rozpoznanie i wyróżnienie kluczowych procesów biznesowych oraz zasobów informatycznych, które są nieodzowne dla bieżącej operacyjności Zamawiającego.
- Realizacja oceny ryzyka i analizy wpływu na działalność (BIA - Business Impact Analysis) z perspektywy ciągłości funkcjonowania organizacji.

2. Projektowanie Polityki Ciągłości Działania:

- Stworzenie strategii mającej na celu zapewnienie nieprzerwanej ciągłości usług ICT, określając cele odnoszące się do czasu przywrócenia działania oraz punktu odzyskiwania danych.
- Zdefiniowanie procedur interwencyjnych, planów awaryjnych oraz procedur odzyskiwania funkcjonalności po wystąpieniu katastroficznych zdarzeń.

3. Integracja z Istniejącymi Systemami Zarządzania:

- Zapewnienie kompleksowej integracji nowo opracowanej polityki z obecnymi systemami zarządzania bezpieczeństwem informacji, zarządzaniem ryzykiem oraz innymi procedurami operacyjnymi, w celu stworzenia spójnego i efektywnego ekosystemu ciągłości działania.

4. Testowanie i Walidacja Polityki:

- Opracowanie i egzekucja testów scenariuszy awaryjnych mających na celu zweryfikowanie efektywności i praktycznej użyteczności formułowanej polityki ciągłości działania.
- Analiza rezultatów testów i modyfikacja polityki w oparciu o zgromadzone dane i obserwacje, celem optymalizacji jej skuteczności.

5. Dokumentacja i Rekomendacje:

- Stworzenie pełnej dokumentacji dotyczącej polityki ciągłości działania, zawierającej detaliczne instrukcje, procedury i wytyczne, które będą stanowić kompendium wiedzy dla Zamawiającego.
- Przedstawienie rekomendacji dotyczących przyszłych działań, potencjalnych udoskonaleń oraz strategii utrzymania gotowości operacyjnej na najwyższym poziomie.

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

CPV 48820000-2 - serwery,
CPV 72268000-1 - usługi dostawy oprogramowania,
CPV 72263000-6 - usługi wdrażania oprogramowania,
CPV 79212000-3 - usługi audytu,
CPV 80550000-4 - usługi szkolenia w dziedzinie bezpieczeństwa.

VII. Miejsce i termin wykonania zamówienia

Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Część 1 będzie realizowana w terminie do 14 dni, część 2 w terminie do 180 dni, liczonego od dnia podpisania umowy w przedmiocie udzielenie zamówienia publicznego.

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

VIII. 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 zawodowej, o ile obowiązek ich posiadania wynika z odrębnych przepisów. Zamawiający nie określa warunku w tym zakresie.

- spełniają warunki udziału w postępowaniu w zakresie sytuacji ekonomicznej lub finansowej. Zamawiający nie określa warunku w tym zakresie.
- spełniają warunki udziału w postępowaniu w zakresie zdolności technicznej lub zawodowej.

2. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. O udzielenie zamówienia publicznego mogą ubiegać się wykonawcy, którzy spełniają warunki udziału w postępowaniu dotyczące zdolności technicznej lub zawodowej:

3.1. Wykonawca spełni warunek udziału w postępowaniu - **dla części 1 zamówienia** – jeśli wykaże, że w okresie ostatnich 3 lat, a jeśli okres prowadzenia działalności jest krótszy, w tym okresie wykonał co najmniej 2 dostawy sprzętu komputerowego o łącznej wartości każdej z dostaw co najmniej 250.000,00 złotych brutto.

Wartości dostaw wyrażone w innej walucie niż PLN należy przeliczyć według średniego kursu walut ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu publikacji ogłoszenia o zamówieniu.

Wykonawcy wspólnie ubiegający się zamówienie muszą wykazać, że co najmniej jeden z nich spełnia powyższy warunek.

3.2. Wykonawca spełni warunek udziału w postępowaniu – **dla części 2 zamówienia** – jeśli wykaże, że:

a) w okresie 5 lat przed złożeniem ofert **zdobył minimum 2-letnie doświadczenie** w prowadzeniu projektów z obszaru cyberbezpieczeństwa. Poprzez prowadzenie projektów z obszaru cyberbezpieczeństwa należy rozumieć wdrożenie systemów teleinformatycznych i/lub SIEM służących poprawie cyberbezpieczeństwa. Do 2-letniego okresu doświadczenia w ramach danego warunku nie wlicza się doświadczenia nabywanego równocześnie na różnych zadaniach w jednym okresie/terminie.

Celem potwierdzenie spełnienia warunku w powyższym zakresie zamawiający wezwie wykonawcę, którego oferta zostanie najwyżej oceniona, do złożenia wykazu usług. Poprzez pojęcie usługi należy rozumieć jedną umowę zawartą z wykonawcą.

b) w okresie 5 lat przed złożeniem ofert **zdobył minimum 2-letnie doświadczenie** w przygotowaniu i prowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń. Do 2-letniego okresu doświadczenia w ramach danego warunku nie

wlicza się doświadczenia nabywanego równocześnie na różnych zadaniach w jednym okresie/terminie.

Celem potwierdzenie spełnienia warunku w powyższym zakresie zamawiający wezwie wykonawcę, którego oferta zostanie najwyżej oceniona, do złożenia wykazu usług. Poprzez pojęcie usługi należy rozumieć jedną umowę zawartą z wykonawcą.

c) dysponuje certyfikowanym audytorem pełniącym rolę Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, posiadającym certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338) w zakresie certyfikacji osób lub równoważny dokument (dopuszcza się inne normy europejskie, które swoim zakresem obejmują normę polską) oraz posiadającym co najmniej 2-letnie doświadczenie jako audytor wiodący systemu zarządzenia bezpieczeństwem informacji (do 2-letniego okresu doświadczenia w ramach danego warunku nie wlicza się doświadczenia nabywanego równocześnie na różnych zadaniach w jednym okresie/terminie) – minimum 1 osoba,

d) dysponuje certyfikowanym audytorem pełniącym rolę Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, posiadającym certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób lub równoważny dokument (dopuszcza się inne normy europejskie, które swoim zakresem obejmują normę polską) oraz posiadającym co najmniej 2-letnie doświadczenie jako audytor wiodący systemu zarządzania ciągłością działania (do 2-letniego okresu doświadczenia w ramach danego warunku nie wlicza się doświadczenia nabywanego równocześnie na różnych zadaniach w jednym okresie/terminie) – minimum 1 osoba.

e) dysponuje **osobami wykonującymi testy penetracyjne infrastruktury** posiadającymi łącznie takie certyfikaty jak: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity), eCPPT (eLearnSecurity) lub równoważne dokumenty i posiadającą co najmniej 2-letnie doświadczenie w zakresie testowania penetracyjnego infrastruktury (do 2-letniego okresu doświadczenia w ramach danego warunku nie wlicza się doświadczenia nabywanego równocześnie na różnych zadaniach w jednym okresie/terminie). Wykonawca sam określa ile

osób wykazuje celem potwierdzenia spełnienia niniejszego warunku – w zależności od posiadanych kwalifikacji tych osób. W przypadku wykazywania więcej niż jednej osoby, każda z wykazanych osób musi posiadać minimum 2-letnie doświadczenie w zakresie testowania penetracyjnego infrastruktury.

f) dysponuje **osobą posiadającą minimum 2-letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń** oraz posiadającą co najmniej jeden z certyfikatów: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity), eCPPT (eLearnSecurity) lub równoważne dokumenty (do 2-letniego okresu doświadczenia w ramach danego warunku nie wlicza się doświadczenia nabywanego równocześnie na różnych zadaniach w jednym okresie/terminie) – minimum 1 osoba.

Wykazanie równoważności z certyfikatami wykazanymi powyżej leży po stronie wykonawcy.

Zamawiający dopuszcza łączenie funkcji dla osób wskazanych powyżej pod warunkiem posiadania wymaganego doświadczenia oraz stosownych certyfikatów lub równoważnych poświadczeń potwierdzających możliwość wykonania zlecenia w każdym z tych obszarów.

Wykonawcy wspólnie ubiegający się o udzielenie zamówienia muszą wykazać, że łącznie spełniają powyższy warunek.

4. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
5. Wykonawca, który polega na zdolnościach innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

IX. Przesłanki wykluczenia wykonawcy

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

1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:

a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,

b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,

c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz.U. z 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 r. 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;

4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

5) 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.

6) 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.

2. Zamawiający nie wprowadza w tym postępowaniu dodatkowych podstaw wykluczenia wskazanych w art. 109 ustawy Pzp.
3. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy Pzp.
4. 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.
5. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia zgodnie z art. 110 ust. 1 ustawy Pzp.
6. 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.

7. Ponadto Zamawiający zastosuje wobec Wykonawców dodatkowe obligatoryjne przesłanki wykluczenia, wynikające z wejścia w życie Ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2024 r. poz. 507).

   Zgodnie z art. 1 pkt 3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, zwanej dalej „ustawą", w celu przeciwdziałania wspieraniu agresji Federacji Rosyjskiej na Ukrainę rozpoczętej w dniu 24 lutego 2022r., wobec osób i podmiotów wpisanych na listę, o której mowa w art. 2 ustawy, stosuje się sankcje polegające m.in. na wykluczeniu z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.

   Na podstawie art. 7 ust. 1 ww. ustawy, z postępowania o udzielenie zamówienia publicznego, prowadzonego na podstawie ustawy Pzp, Zamawiający wyklucza:

   1) wykonawcę wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
   2) wykonawcę, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
   3) wykonawcę, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2024 r. poz. 619), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

   W przypadku wykonawcy wykluczonego na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r., zamawiający odrzuca ofertę takiego wykonawcy. Ponadto

zamawiający, w ramach weryfikacji przesłanek wykluczenia, o których mowa powyżej, zastrzega możliwość wezwania wykonawcy do złożenia wyjaśnień.

X. Obowiązek zatrudnienia na podstawie stosunku pracy

Nie dotyczy

XI. Wykaz oświadczeń i 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:

   1.1.1. potwierdzających spełnienie warunków udziału w postępowaniu (dla części 1 zamówienia): wykazu dostaw wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, 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 lub są wykonywane oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy (w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje lub inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy) – wzór wykazu dostaw stanowi załącznik nr 4 do SWZ,

   1.1.2. potwierdzających spełnienie warunków udziału w postępowaniu (dla części 2 zamówienia):

   - wykazu usług wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 5 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich przedmiotu, dat

wykonania i podmiotów, na rzecz których usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje lub inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy – wzór wykazu usług stanowi załącznik nr 5 do SWZ,

- wykazu osób skierowanych przez wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług wraz z informacjami na temat ich kwalifikacji zawodowych i doświadczenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tą osobą – wzór wykazu osób stanowi załącznik nr 6 do SWZ.

1.2. potwierdzających brak podstaw do wykluczenia z udziału w postępowaniu:

1.2.1. oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Prawo zamówień publicznych, w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w:

- art. 108 ust. 1 pkt 3 ustawy;
- art. 108 ust. 1 pkt 4 ustawy, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego;
- art. 108 ust. 1 pkt 5 ustawy, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji;
- art. 108 ust. 1 pkt 6 ustawy,

1.2.2. zamawiający zamiast podmiotowych środków dowodowych w postaci informacji z Krajowego Rejestru Karnego w zakresie:

- art. 108 ust 1 pkt 1 i 2 ustawy Pzp,
- art. 108 ust 1 pkt 4 ustawy Pzp, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego, żąda oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust 1 ustawy.

2. Na wezwanie zamawiającego każdy z wykonawców wspólnie ubiegających się o zamówienie przedkłada również dokumenty określone w ust. 1 punkt 1.2. Dokumenty określone w ust 1 pkt 1.1.1 i 1.1.2. składa ten z wykonawców wspólnie ubiegających się o zamówienie, który wykazuje spełnienie warunków udziału w postępowaniu.

3. Zamawiający nie wezwie Wykonawcy do złożenia podmiotowych środków dowodowych, jeżeli: może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile wykonawca wskazał w Oświadczeniu o braku podstaw wykluczenia i spełnianiu warunków udziału w postępowaniu, dane umożliwiające dostęp do tych środków.

4. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

5. **Zamawiający wymaga od Wykonawcy złożenia wraz z ofertą następujących przedmiotowych środków dowodowych w celu potwierdzenia zgodności oferowanych usług z wymaganiami Zamawiającego w zakresie wskazanym w zestawieniu poniżej:**
dla części 2 zamówienia; co najmniej dwa z trzech certyfikatów: Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE), Certified Professional Penetration Tester (eCPPTv2) w zakresie testowania I weryfikacji poprawności wdrażanych rozwiązań.
Jeśli powyższe certyfikaty wydane są imiennie dla osoby, to ta osoba musi bezpośrednio wykonywać zamówienie w danym zakresie. Tam gdzie certyfikaty są imienne wykonawca musi wraz z ofertą złożyć również wykaz osób wraz z ich doświadczeniem, potwierdzających doświadczenie każdej z tych osób w okresie minimum 2 lat w ramach certyfikowanego obszaru.
Zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeżeli potwierdzają one, że oferowane usługi spełniają określony przez zamawiającego wymagany zakres.

6. 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.

7. Postanowień punktu 6 powyżej 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.

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

XII. Podwykonawstwo (dotyczy 1 i 2 części zamówienia)

1. Zamawiający nie wprowadza zastrzeżenia wskazującego na obowiązek osobistego wykonania przez wykonawcę kluczowych części zamówienia. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.

2. Zamawiający żąda wskazania przez wykonawcę, w ofercie, części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, oraz podania przez wykonawcę nazw ewentualnych podwykonawców, jeżeli są już znani.

3. Pozostałe wymagania dotyczące podwykonawców zostały określone w projektowanych postanowieniach umowy.

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

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

   1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;

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

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

6. 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.
7. 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.
8. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia oświadczenia podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.

XIV. Kryteria równoważności

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 SWZ, 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 przygotowania ofert oraz dokumentów wymaganych przez zamawiającego

1. **Oferta oraz podmiotowe środki dowodowe składane elektronicznie muszą zostać podpisane w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub w postaci elektronicznej opatrzonej elektronicznym podpisem zaufanym lub elektronicznym podpisem osobistym**.
2. **W procesie składania oferty, w tym podmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny lub elektroniczny podpis zaufany lub elektroniczny podpis osobisty Wykonawca składa bezpośrednio na dokumencie, który następnie przesyła do systemu.**
3. Oferta powinna być:

1) sporządzona ściśle według wymagań określonych w niniejszej SWZ, tj. wg wzoru Formularza oferty, stanowiącego **załącznik Nr 1** do SWZ. W przypadku gdy Wykonawca nie skorzysta z przygotowanego przez Zamawiającego wzoru Formularza oferty, oferta powinna zawierać wszystkie informacje wymagane we wzorze Formularza oferty,
2) złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
3) podpisana **kwalifikowanym podpisem elektronicznym** lub **elektronicznym podpisem zaufanym** lub **elektronicznym podpisem osobistym** przez osobę/osoby upoważnioną/upoważnione.

4. Każdy z Wykonawców może złożyć tylko **jedną ofertę na każdą część**. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje, że oferta podlegać będzie odrzuceniu.
5. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim i zostać wypełnione przez Wykonawcę w zgodnej z niniejszą SWZ formie. Zamawiający dopuszcza złożenie przedmiotowych środków dowodowych w językach obcych, przy czym wykonawca powinien złożyć je wraz z tłumaczeniem na język polski.
6. Jeżeli w imieniu wykonawcy/wykonawcy wspólnie ubiegającego się o zamówienie/podmiotu udostępniającego zasoby działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów rejestrowych (KRS, CEiDG lub innego właściwego rejestru), wykonawca dołącza do oferty pełnomocnictwo. Treść pełnomocnictwa musi jednoznacznie wskazywać czynności, do wykonywania których

pełnomocnik jest upoważniony.

7. Pełnomocnictwo do złożenia oferty także przekazuje się w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
8. W przypadku gdy pełnomocnictwo do złożenia oferty lub oświadczenia, o których mowa powyżej, zostało sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone podpisem kwalifikowanym, potwierdzającym zgodność odwzorowania cyfrowego z dokumentem w postaci papierowej. Odwzorowanie cyfrowe pełnomocnictwa powinno potwierdzać prawidłowość umocowania na dzień złożenia oferty lub ww. oświadczeń. Poświadczenia zgodności cyfrowego odwzorowania pełnomocnictwa z dokumentem w postaci papierowej dokonuje mocodawca. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej może dokonać również notariusz.
9. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia **(konsorcja, spółki cywilne)** do oferty należy załączyć pełnomocnictwo dla pełnomocnika (Lidera) do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
10. Dokumenty lub oświadczenia, o których mowa w rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. z 2020 r. poz. 2415 z późn. zm.), zwany dalej „rozporządzeniem” składane przez wykonawcę i podmiot udostępniający zasoby, na zdolnościach lub sytuacji których polega wykonawca na zasadach określonych w art. 118 ustawy Prawo zamówień publicznych, sporządza się **w formie elektronicznej opatrzone kwalifikowanym podpisem elektronicznym lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym lub elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem**.
11. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy Prawo zamówień publicznych lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach

określonych w art. 118 ustawy Prawo zamówień publicznych, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania”, **zostały wystawione przez upoważnione podmioty** inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby, zwane dalej „upoważnionymi podmiotami”, **jako dokument elektroniczny, przekazuje się ten dokument**.

12. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy Prawo zamówień publicznych lub dokumenty potwierdzające umocowanie do reprezentowania, **zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu** opatrzone kwalifikowanym podpisem elektronicznym, a w przypadku postępowań lub konkursów o wartości mniejszej niż progi unijne, kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, **poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej**.
13. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w punkcie **11** powyżej, dokonuje w przypadku:
    1) podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania – odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą,
    2) przedmiotowych środków dowodowych – odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia,
    3) innych dokumentów, w tym dokumentów, o których mowa w art. 94 ust 2 ustawy Prawo zamówień publicznych – odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.

    14. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w punkcie **11** powyżej, może dokonać również notariusz.
15. 1. Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy Prawo zamówień publicznych, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty, oraz

pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, a w przypadku postępowań lub konkursów o wartości mniejszej niż progi unijne, kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

2. W przypadku gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy Prawo zamówień publicznych, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, a w przypadku postępowań lub konkursów, o wartości mniejszej niż progi unijne, kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.

3. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w punkcie 2 powyżej, dokonuje w przypadku:

1) podmiotowych środków dowodowych – odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą,
2) przedmiotowego środka dowodowego, dokumentu, o którym mowa w art. 94 ust. 2 ustawy, oświadczenia, o którym mowa w art. 117 ust. 4 ustawy Prawo zamówień publicznych, lub zobowiązania podmiotu udostępniającego zasoby – odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia,
3) **pełnomocnictwa – mocodawca**.

4. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w punkcie 2 powyżej, może dokonać również notariusz.

16. Przez cyfrowe odwzorowanie, o którym mowa w punktach 12, 13 i 14 oraz w punkcie 15 podpunkty od 2 do 4 należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.

17. Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii, wyłącznie wtedy, gdy złożona kopia jest nieczytelna lub budzi wątpliwości co do jej prawdziwości.

18. Podpisy kwalifikowane wykorzystywane przez Wykonawców do podpisywania wszelkich plików muszą spełniać "Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku".
19. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny, Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików XAdES.
20. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli Wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
21. Wykonawca, za pośrednictwem https://platformazakupowa.pl może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem:
https://platformazakupowa.pl/strona/instrukcje-wykonawca
22. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.
23. **Rozszerzenia plików wykorzystywanych przez Wykonawców muszą być zgodne z** Załącznikiem nr 2 do "Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych", zwanego dalej Rozporządzeniem KRI.
24. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .docx .xls .xlsx .jpg (.jpeg)

ze szczególnym wskazaniem na .pdf

25. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z rozszerzeń:
    1) .zip
    2) .7Z

26. Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi **maksymalnie 10MB**, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi **maksymalnie 5MB**.
27. W przypadku stosowania przez wykonawcę kwalifikowanego podpisu elektronicznego:

1) Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu zamawiający zaleca, w miarę możliwości, **przekonwertowanie plików składających się na ofertę na rozszerzenie .pdf i opatrzenie ich podpisem kwalifikowanym w formacie PAdES.**
2) Pliki w innych formatach niż PDF **zaleca się opatrzyć podpisem w formacie XAdES o typie zewnętrznym**. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
3) Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.

28. Zamawiający zaleca aby **w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju.** Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
29. Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
30. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
31. Jeśli Wykonawca pakuje dokumenty np. w plik o rozszerzeniu .zip, zaleca się wcześniejsze podpisanie każdego ze skompresowanych plików.
32. Zamawiający zaleca aby **nie** wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty.
33. **Kompletna oferta musi zawierać następujące, aktualne na dzień złożenia, dokumenty:**

1) **formularz Oferty**, sporządzony na podstawie wzoru stanowiącego **załącznik nr 1** do SWZ;
2) **pełnomocnictwo** do podpisania oferty (jeżeli dotyczy);

3) **pełnomocnictwo** do reprezentowania Wykonawców wspólnie ubiegających się o udzielenie zamówienia (jeżeli dotyczy);
4) **wykonawca dołącza do oferty oświadczenie** o braku podstaw wykluczenia i spełnianiu warunków udziału w postępowaniu, w zakresie wskazanym przez Zamawiającego, zgodnie z **załącznikiem 2** do SWZ. Przedmiotowe oświadczenie stanowi dowód potwierdzający brak podstaw wykluczenia i spełnianie warunków udziału w postępowaniu na dzień składania ofert, tymczasowo zastępujący wymagane przez Zamawiającego podmiotowe środki dowodowe.
5) **W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie, o którym mowa w pkt 4, składa każdy z wykonawców, także zgodnie z załącznikiem nr 2** do SWZ. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
6) **W przypadku polegania przez Wykonawcę na zdolnościach lub sytuacji podmiotów udostępniających zasoby, wykonawca przedstawia, wraz z oświadczeniem, o którym mowa w pkt 4, także oświadczenie podmiotu udostępniającego zasoby,** potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu w zakresie, w jakim wykonawca powołuje się na jego zasoby (treść oświadczenia znajduje się na formularzu Zobowiązania – **załącznik Nr 3** do SWZ.
7) **zobowiązanie podmiotu** do udostępnienia zasobów i oświadczenie tego podmiotu o braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu **(jeżeli Wykonawca polega na zasobach podmiotu udostępniającego zasoby)**, wg wzoru stanowiącego **załącznik nr 3** do SWZ (jeżeli dotyczy),
8) **przedmiotowe środki dowodowe, o których mowa w punkcie XI podpunkt 5 (dla części 2 zamówienia).**

34. Ofertę wraz z oświadczeniami i dokumentami należy złożyć w terminie do dnia 29.11.2024 r. do godziny 10:00 za pośrednictwem platformazakupowa.pl pod adresem: https://platformazakupowa.pl/transakcja/1008070

35. Otwarcie ofert nastąpi niezwłocznie po upływie terminu składania ofert, tj. dnia 29.11.2024 r. o godzinie 10:30.

36. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po

usunięciu awarii.

37. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

38. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

39. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:

1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte;
2) cenach lub kosztach zawartych w ofertach.

40. Wykonawca nie może wprowadzić zmian do złożonej oferty.

41. Wykonawca może przed upływem terminu składania ofert wycofać ofertę.

XVI. Informacja dla wykonawców wspólnie ubiegających się o zamówienie

1. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia

1) Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.
2) W przypadku, o którym mowa w pkt 1, Wykonawcy ustanawiają Pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
3) Zaleca się, aby Pełnomocnikiem był jeden z Wykonawców wspólnie ubiegających się o udzielenie zamówienia; Wszelka korespondencja prowadzona będzie wyłącznie z Pełnomocnikiem.
4) 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 roboty budowlane lub usługi, do realizacji których te zdolności są wymagane. W takim przypadku wykonawcy wspólnie ubiegający się o udzielenie zamówienia **wskazują w treści oferty oświadczenie**, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy.
5) Oferta musi być podpisana w taki sposób, by poprawnie zobowiązywała wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

6) Jeżeli w postępowaniu zostanie wybrana oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego, kopii umowy regulującej współpracę tych Wykonawców.
7) Zamawiający nie zastrzega obowiązku osobistego wykonania, przez poszczególnych wykonawców wspólnie ubiegających się o udzielenie zamówienia, kluczowych zadań dotyczących zamówień na roboty budowlane lub usługi.
8) Przepisy dotyczące wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia.
9) Wykonawcy wspólnie ubiegający się o udzielenie zamówienia, ponoszą solidarną odpowiedzialność za wykonanie umowy i wniesienie zabezpieczenia należytego wykonania umowy.
10) Wypełniając formularz oferty należy wpisać dane (nazwa, adres itd.) Pełnomocnika (Lidera) oraz wszystkich Wykonawców wspólnie ubiegających się o zamówienie. W innych dokumentach (załączniki) powołujących się na Wykonawcę w miejscu np. nazwa, adres Wykonawcy, należy wpisać dane dotyczące Pełnomocnika (Lidera) i Wykonawcy, którego dany dokument (załącznik) dotyczy.

XVII. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty

1. **Przy wyborze oferty w zakresie Części 1 zamawiający będzie się kierował następującymi kryteriami:**

   Cena – 100 punktów

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

   Przy ocenie ofert w zakresie Części 1 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 of x 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.

Wszystkie obliczenia w zakresie kryterium oceny ofert dla części 1 dokonywane będą z dokładnością do dwóch miejsc po przecinku.

W związku z zaistnieniem przesłanki o której mowa w art. 246 ust. 2 PZP możliwe było zastosowanie dla części 1 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.

2. **Przy wyborze oferty w zakresie Części 2 Zamawiający będzie się kierował następującymi kryteriami:**

   Cena – 100 punktów

Przy wyborze oferty dla Części 2 Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższego kryterium, jest ofertą najkorzystniejszą.

Przy ocenie ofert dla Części 2 w kryterium „Cena” (C) punkty zostaną przyznane w poniższy sposób:

Cena – znaczenie 100% (maksymalnie 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 of x 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.

Wszystkie obliczenia w zakresie kryterium oceny ofert dla części 2 dokonywane będą z dokładnością do dwóch miejsc po przecinku.

W związku z zaistnieniem przesłanki o której mowa w art. 246 ust. 2 PZP możliwe było zastosowanie dla części 2 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. Zamawiający określił wymagania wobec wykonawcy i osób wykonujących usługi posiadające wysokie kwalifikacje i doświadczenie w obszarze cyberbezpieczeństwa co zostaje poparte m.in. przedmiotowymi środkami dowodowymi.

XVIII. Projektowane podstawienia umowy w sprawie zamówienia publicznego

Projektowane postanowienia umowy w sprawie zamówienia publicznego określone zostały w **załączniku nr 7a i 7b** do SWZ.

XIX. RODO

Złożenie oferty stanowi wyraźne działanie potwierdzające wyrażenie zgody przez wykonawcę na przetwarzanie wszystkich tych danych osobowych zawartych w jego ofercie, których przetwarzanie nie może być realizowane przez zamawiającego w oparciu o inne podstawy przetwarzania określone w art. 6.1 RODO.

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Urząd Miejski w Grodkowie, ul. Warszawska 29, 49-200 Grodków;
2. Inspektorem ochrony danych w Urzędzie Miejskim w Grodkowie jest Agata Wagner iod@grodkow.pl;
3. Pani/Pana dane osobowe przetwarzane będą w celu przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego, udzielenia zamówienia, prowadzenia dokumentacji księgowo-podatkowej, archiwizacji danych oraz dochodzenia roszczeń lub obrony przed roszczeniami.
4. Podstawą przetwarzania danych osobowych jest:
   1) ustawa z 11.09.2019 r. – Prawo zamówień publicznych;

2) ustawa z 27.08.2009 r. o finansach publicznych;
3) ustawa z 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach;
4) art. 6 pkt.1 lit. c RODO
– przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

5. Odbiorcami Pani/Pana danych osobowych będą podmioty upoważnione na podstawie zawartych umów powierzenia oraz uprawnione na mocy obowiązujących przepisów prawa, w szczególności osoby lub podmioty, którym zostanie udostępniona dokumentacja postępowania na podstawie art. 18 oraz art. 74-76 ustawy Pzp. Zasada jawności ma zastosowanie do wszystkich danych osobowych, z wyjątkiem danych, o których mowa w art. 9 ust. 1 RODO (szczególna kategoria danych).
6. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji celu przetwarzania oraz przez okres wynikający z przepisów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, w szczególności zgodnie art. 78 ust. 1 i 4 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli okres obowiązywania umowy w sprawie zamówienia publicznego przekracza 4 lata – przez cały okres obowiązywania umowy.
7. Posiada Pani/Pan prawo do:
   1) żądania dostępu do danych; w przypadku gdy wykonanie tego obowiązku, wymagałoby niewspółmiernie dużego wysiłku, zamawiający może, zgodnie z art. 75 ustawy Pzp, żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia;
   2) żądania sprostowania lub uzupełnienia danych osobowych; zgodnie z art. 76 ustawy Pzp wykonanie tego obowiązku nie może naruszać integralności protokołu postępowania oraz jego załączników;
   3) usunięcia danych w przypadku, gdy dane osobowe nie są już niezbędne do celów, w których zostały zebrane, lub w inny sposób przetwarzane;
   4) żądania ograniczenia przetwarzania danych osobowych; zgodnie z art. 74 ust. 3 ustawy Pzp wykonanie tego obowiązku nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie

zamówienia.

5) wniesienia skargi do organu nadzorczego, tj. Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-913 Warszawa.

8. Nie przysługuje Pani/Panu:
   a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.
9. Pani/Pana dane osobowe nie będą poddawane zautomatyzowanemu podejmowaniu decyzji, w tym również profilowaniu.
10. Pani/Pana dane osobowe nie będą przekazywane do państw trzecich.
11. Podanie danych osobowych jest wymogiem ustawowym określonym w przepisach Pzp, związanych z udziałem w postępowaniu o udzielenie zamówienia; konsekwencje niepodania określonych danych wynikają z ustawy Pzp.
12. Jednocześnie Zamawiający przypomina o ciążącym na Pani/Panu 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.

XX. Informacja o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzenia, wysyłania i odbierania korespondencji elektronicznej

1. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem https://platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/grodkow lub bezpośrednio pod adresem przedmiotowego postępowania: https://platformazakupowa.pl/transakcja/1008070

2. Komunikacja między Zamawiającym a Wykonawcami w zakresie:

a) przesyłania Zamawiającemu pytań do treści SWZ;
b) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia podmiotowych środków dowodowych;
c) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia/ poprawienia/ uzupełnienia oświadczenia, o którym mowa w art. 125 ust. 1, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu;
d) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu;
e) przesłania odpowiedzi na inne wezwania Zamawiającego wynikające z ustawy - Prawo zamówień publicznych;
f) przesyłania wniosków, informacji, oświadczeń Wykonawcy;
g) przesyłania odwołania/inne

odbywa się za pośrednictwem https://platformazakupowa.pl i formularza **„Wyślij wiadomość do zamawiającego".**

Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem https://platformazakupowa.pl poprzez kliknięcie przycisku **„Wyślij wiadomość do zamawiającego",** po których pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.

3. W sytuacjach awaryjnych w szczególności w przypadku braku działania platformy zakupowej https://platformazakupowa.pl, Zamawiający dopuszcza także komunikację za pośrednictwem poczty elektronicznej, na adres: pm@grodkow.pl, z zastrzeżeniem, że Ofertę Wykonawca może złożyć wyłącznie za pośrednictwem https://platformazakupowa.pl

4. Zamawiający będzie przekazywał Wykonawcom informacje w formie elektronicznej za pośrednictwem https://platformazakupowa.pl Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w zakładce **"Wiadomości – komunikaty publiczne"**. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana w formie elektronicznej za

pośrednictwem https://platformazakupowa.pl do konkretnego Wykonawcy za pośrednictwem zakładki **„Wiadomości – wiadomości prywatne”**.

5. Zamawiający nie przewiduje sposobu komunikowania się z wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej wskazanych w SWZ.

6. Wykonawca jako uczestnik postępowania ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na https://platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.

7. Zamawiający, zgodnie z Rozporządzeniem 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, określa niezbędne wymagania sprzętowo-aplikacyjne umożliwiające pracę na https://platformazakupowa.pl, tj.

a) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
b) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
c) zainstalowana dowolna, inna przeglądarka internetowa niż Internet Explorer,
d) włączona obsługa JavaScript,
e) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
f) Szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.
g) Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.

8. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:

a) akceptuje warunki korzystania z https://platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej https://platformazakupowa.pl w zakładce **„Regulamin”** oraz uznaje go za wiążący,
b) zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej na stronie https://platformazakupowa.pl

9. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z https://platformazakupowa.pl**,** w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce **„Wyślij wiadomość do zamawiającego”**).

10. Zamawiający informuje, że instrukcje korzystania z https://platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu https://platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/instrukcje-wykonawca

11. Oferta oraz podmiotowe środki dowodowe składane elektronicznie muszą zostać podpisane w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub w postaci elektronicznej opatrzonej elektronicznym podpisem zaufanym lub elektronicznym podpisem osobistym.

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

13. Zamawiający będzie odpowiadał na zapytania wykonawców wysyłając wiadomość publiczną zamieszczoną w dziale **„Komunikaty”** na stronie internetowej https://platformazakupowa.pl/pn/grodkow/proceedings

14. W wyjątkowych przypadkach (np. w sytuacjach awaryjnych – braku działania strony internetowej https://platformazakupowa.pl/ , Zamawiający może również komunikować się z wykonawcami za pomocą adresu elektronicznego pm@grodkow.pl

15. Zamawiający prosi o przekazywanie pytań również w formie edytowalnej, gdyż skróci to czas udzielania wyjaśnień.

16. Zamawiający jest zobowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem że wniosek o wyjaśnienie treści SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.

17. Jeżeli zamawiający nie udzieli wyjaśnień w powyższym terminie, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert.

18. W przypadku gdy wniosek o wyjaśnienie treści SWZ wpłynął później niż na 4 dni przed upływem terminu składania ofert, zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużania terminu składania ofert.

19. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.

20. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert, zmienić treść SWZ. W przypadku gdy zmiana treści SWZ jest istotna dla sporządzenia oferty lub wymaga od wykonawców dodatkowego czasu na zapoznanie się ze zmianą treści SWZ i przygotowanie ofert, Zamawiający przedłuża termin składania ofert o czas niezbędny na ich przygotowanie.

21. Dokonaną zmianę treści SWZ Zamawiający udostępnia na stronie internetowej postępowania https://platformazakupowa.pl/pn/grodkow/proceedings.

22. Zmiany są każdorazowo wiążące dla Wykonawców.

23. Ofertę składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa następnie wraz z plikami stanowiącymi jawną część należy ten plik zaszyfrować.

24. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

XXI. Sposób obliczenia ceny

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

XXII. Informacja o formalnościach, jakie muszą został dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający zawiera umową w sprawie zamówienia publicznego, z uwzględnieniem art. 577 pzp, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umową w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertą.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o miejscu i terminie podpisania umowy.
4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią załącznik 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.

XXIII. 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 oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia 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 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 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 6 i 7 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.

XXIV. Zabezpieczenie należytego wykonania umowy

(dotyczy części 1 i części 2 zamówienia)

1. **Informacje ogólne.**

   Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy. Zabezpieczenie służy także do pokrycia roszczeń Zamawiającego z tytułu rękojmi za wady.

2. **Wysokość zabezpieczenia należytego wykonania umowy.**

   Zamawiający będzie żądał od Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, wniesienia najpóźniej w dniu podpisania umowy zabezpieczenia należytego wykonania umowy w wysokości **3 % ceny całkowitej podanej w ofercie.**

3. **Forma zabezpieczenia należytego wykonania umowy.**

   1) Zabezpieczenie należytego wykonania umowy może być wniesione według

wyboru Wykonawcy w jednej lub w kilku następujących formach:

a) pieniądzu;
b) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo- kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;
c) gwarancjach bankowych;
d) gwarancjach ubezpieczeniowych;
e) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.

2) Zabezpieczenie wnoszone w pieniądzu Wykonawca wpłaci przelewem na następujący rachunek bankowy Zamawiającego: **51 1020 3668 0000 5102 0015 7792**

3) Jeżeli zabezpieczenie wniesiono w pieniądzu, Zamawiający przechowuje je na oprocentowanym rachunku bankowym. Zamawiający zwraca zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.

4) W przypadku składania zabezpieczenia w formie gwarancji lub poręczenia, gwarancja winna być sporządzona zgodnie z obowiązującym prawem i winna zawierać zobowiązanie do „zapłacenia kwoty gwarancji/poręczenia na pierwsze pisemne żądanie Zamawiającego”.

5) Zabezpieczenie wnoszone w formie gwarancji lub poręczenia ma być dostarczone w formie oryginału, w wersji papierowej bądź elektronicznej przez wykonawcę, do siedziby zamawiającego, najpóźniej do chwili podpisania umowy.

6) Treść oświadczenia zawartego w gwarancji lub w poręczeniu musi zostać zaakceptowana przez zamawiającego przed podpisaniem umowy.

7) W trakcie realizacji umowy wykonawca może dokonać zmiany formy zabezpieczenia na jedną lub kilka form, o których mowa w pkt. 1). Zmiana formy zabezpieczenia jest dokonywana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości.

8) W przypadku wniesienia wadium w pieniądzu, Wykonawca może wyrazić zgodę na zaliczenie kwoty wadium na poczet zabezpieczenia.

4. Zwrot zabezpieczenia należytego wykonania umowy.

Zamawiający dokona zwrotu zabezpieczenia należytego wykonania umowy w następujący sposób:

1) 70% wartości zabezpieczenia zostanie zwrócone w terminie 30 dni od dnia wykonania zamówienia i uznania przez zamawiającego za należycie wykonane;
2) 30% wartości zabezpieczenia Zamawiający pozostawi na zabezpieczenie roszczeń z tytułu rękojmi za wady lub gwarancji – kwota ta zostanie zwrócona nie później niż w 15 dniu po upływie okresu rękojmi za wady lub gwarancji.
   Dla części 2 zamówienia kwota zostanie zwrócona nie później niż w 15 dniu licząc od końca upływu terminu trwałości projektu, tj. nie później niż w dniu 15.07.2026 r.

XXV. Osoby uprawnione do kontaktowania się z wykonawcami

W zakresie merytorycznym: Dariusz Świerczyński: tel. 77/ 40 40 342.

W zakresie procedury: Barbara Łabuz: tel. 77/ 40 40 308.

XXVI. Spis załączników

Załącznik nr 1 Formularz oferty

Załącznik nr 2 Oświadczenie wykonawcy

Załącznik nr 3 Oświadczenie podmiotu udostępniającego wraz z zobowiązaniem

Załącznik nr 4 Wykaz dostaw

Załącznik nr 5 Wykaz usług

Załącznik nr 6 Wykaz osób

Załącznik nr 7a Projektowane postanowienia umowy dla części 1 zamówienia

Załącznik nr 7b Projektowane postanowienia umowy dla części 2 zamówienia