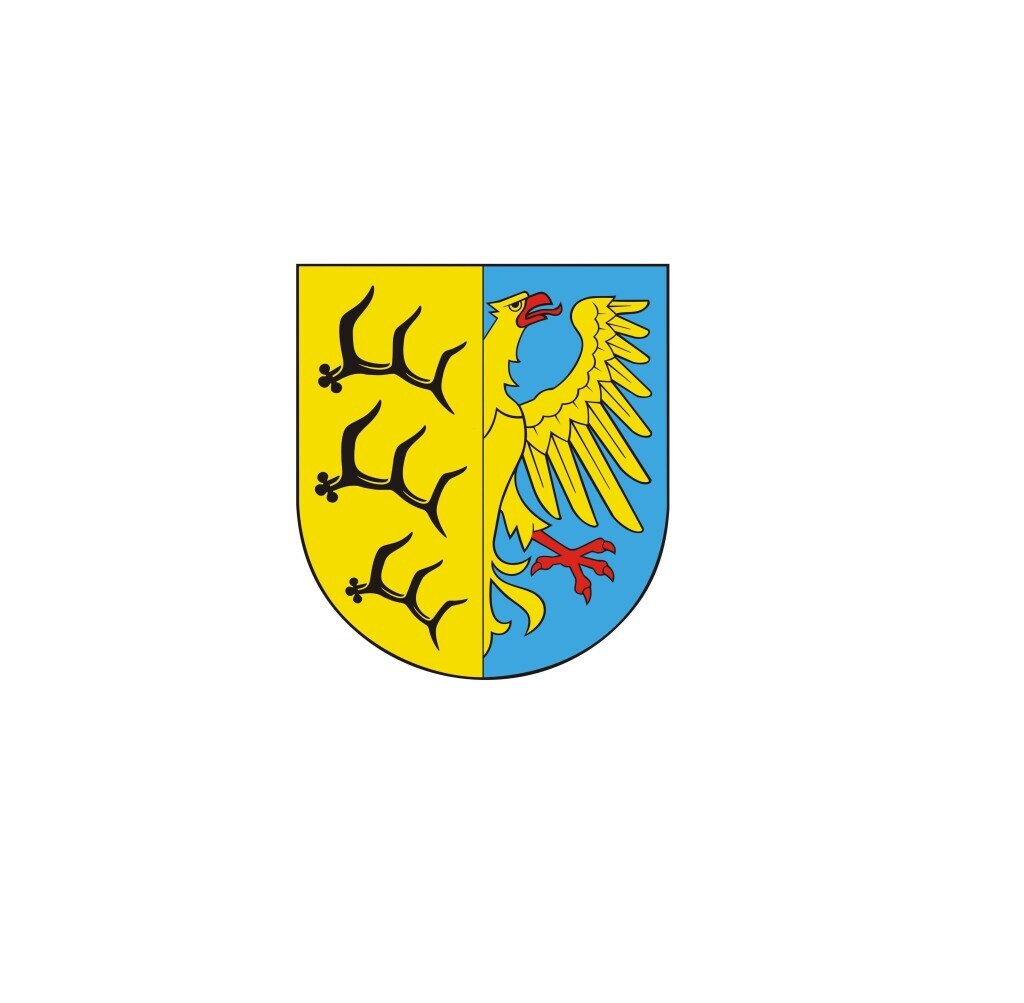
Znak referencyjny: ST.I.271.16.2025

V 2.0

****

**SPECYFIKACJA WARUNKÓW ZAMÓWIENIA**

**(Nr referencyjny: ST.I.271.16.2025)**

**w postępowaniu o udzielenie zamówienia publicznego pn.:**

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

Spis treści

[I ZAMAWIAJĄCY 3](#_Toc214617298)

[II Definicje 4](#_Toc214617299)

[III Wartość zamówienia 5](#_Toc214617300)

[IV Uzasadnienie braku podziału zamówienia na części 5](#_Toc214617301)

[V Tajemnica przedsiębiorstwa 6](#_Toc214617302)

[VI Wymagania dotyczące wadium 7](#_Toc214617303)

[VII Opis przedmiotu zamówienia 7](#_Toc214617304)

[VIII Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV) 52](#_Toc214617305)

[IX Miejsce i Terminy wykonania zamówienia 52](#_Toc214617306)

[X Warunki udziału w postępowaniu 52](#_Toc214617307)

[XI Przesłanki wykluczenia Wykonawcy 53](#_Toc214617308)

[XII Obowiązek zatrudniania przez wykonawcę osób na podstawie stosunku pracy (art. 95 PZP) 55](#_Toc214617309)

[XIII Wykaz oświadczeń lub dokumentów, jakie mają złożyć wykonawcy w celu wykazania spełniania warunków udziału w postępowaniu oraz niepodlegania wykluczeniu z postępowania 56](#_Toc214617310)

[XIV Podwykonawcy 57](#_Toc214617311)

[XV Informacja dla wykonawców polegających na zasobach innych podmiotów, na zasadach określonych w art. 118 ustawy PZP 57](#_Toc214617312)

[XVI Kryterium równoważności 59](#_Toc214617313)

[XVII Opis sposobu składania ofert w postępowaniu 59](#_Toc214617314)

[XVIII Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem wag tych kryteriów i sposobu oceny ofert 60](#_Toc214617315)

[XIX Wzór umowy 61](#_Toc214617316)

[XX RODO 61](#_Toc214617317)

[XXI Informacje Dodatkowe 62](#_Toc214617318)

[XXII Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej 62](#_Toc214617319)

[XXIII Sposób obliczenia ceny 65](#_Toc214617320)

[XXIV Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego 65](#_Toc214617321)

[XXV Środki ochrony prawnej 66](#_Toc214617322)

[ZAŁĄCZNIKI 68](#_Toc214617323)

# I ZAMAWIAJĄCY

Gmina Pokój zwana dalej „Zamawiającym”

ul. Sienkiewicza 8, 46 – 034 Pokój

NIP: 752-13-59-322 , Regon: 531412740

Nr telefonu: 77 469 30 97

Poczta elektroniczna [e-mail]: zamowieniapubliczne@gminapokoj.pl

Strona internetowa Zamawiającego [URL]: www.bip.gminapokoj.pl

Godziny urzędowania: poniedziałek- piątek od 7:30 do 15:30 z wyłączeniem dni ustawowo wolnych od pracy.

Adres strony internetowej prowadzonego **postępowania:** **https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-2c88c41b-7035-4e86-a21c-21923619c95e**

Identyfikator (ID) postępowania na Platformie **e-Zamówienia: ocds-148610-2c88c41b-7035-4e86-a21c-21923619c95e**

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 z późn. zm.) oraz aktów wykonawczych wydanych na jej podstawie.

**Tryb prowadzonego postępowania**

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

**Termin związania ofertą**

Wykonawca jest związany ofertą do dnia **27.01.2026**

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

# II Definicje

Zamawiający dokonał opisu przedmiotu z wykorzystaniem następujących definicji:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Termin** | **Definicje** |
| 1. | **OPZ** | Opis przedmiotu zamówienia |
| 2. | **Umowa** | Należy przez to rozumieć umowę zawartą między zamawiającym a jednym lub większą liczbą wykonawców, której celem jest ustalenie warunków dotyczących zamówień, jakie mogą zostać udzielone w danym okresie, w szczególności cen i, jeżeli zachodzi taka potrzeba, przewidywanych ilości |
| 3. | **Zamawiający** | Należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, obowiązaną na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych do jej stosowania. |
| 4. | **Wykonawca** | należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która oferuje na rynku wykonanie robót budowlanych lub obiektu budowlanego, dostawę produktów lub świadczenie usług lub ubiega się o udzielenie zamówienia, złożyła ofertę lub zawarła umowę w sprawie zamówienia publicznego. |
| 5. | **Platforma e-zamówienia** | ogólnodostępne i nieodpłatne narzędzie informatyczne do obsługi postępowań o udzielenie zamówienia publicznego w tym przedmiotowego postepowania, w szczególności do elektronicznego składania ofert dostępne pod adresem: https://ezamowienia.gov.pl |
| 6. | **Kwalifikowalny podpis elektroniczny** | podpis wystawiony przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny, spełniający wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 422). |
| 7. | **RODO** | rozporządzenie 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), |
| 8. | **podpis zaufany** | podpis elektroniczny, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji, zawierający dane identyfikujące osobę tj. imię (imiona), nazwisko, PESEL, ustalone na podstawie środka identyfikacji elektronicznej, identyfikator środka identyfikacji elektronicznej, przy użyciu, którego został złożony, czas jego złożenia, |
| 9. | **podpis osobisty** | zaawansowany podpis elektroniczny w rozumieniu art. 3 pkt 11 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE, weryfikowany za pomocą certyfikatu podpisu osobistego |

# III Wartość zamówienia

1. Szacunkowa wartość zamówienia nie przekracza wyrażoną w złotych równowartość kwoty określonej w przepisach wydanych na podstawie ustawy prawo zamówień publicznych z dnia 11 września 2019 r. (dz.u. z 2024 r. poz. 1320 z późn. Zm. ).

# IV Uzasadnienie braku podziału zamówienia na części

Zamówienie objęte niniejszym postępowaniem nie zostało podzielone na części. Zamawiający nie dopuszcza możliwości składania ofert częściowych w ramach przedmiotowego zamówienia.

Wartość zamówienia jest niższa od tzw. progów unijnych które zobowiązują do implementacji dyrektyw UE. Dyrektywa 2014/24/UE w treści motywu 78 wskazuje, że aby zwiększyć konkurencję, instytucje zamawiające powinny w szczególności zachęcać do dzielenia dużych zamówień na części. Przedmiotowe zamówienie nie jest dużym zamówieniem w rozumieniu motywu 78 powołanej dyrektywy UE (dyrektywy stosuje się od tzw. progów UE, a dyrektywa posługuje się pojęciem dużego zamówienia na gruncie zamówień podlegających dyrektywie, a więc zamówienia o wartości znacznie przewyższającej tzw. progi UE).

Należy podkreślić, że dostarczone oprogramowanie musi być kompatybilne z oferowanym sprzętem komputerowym oraz urządzeniami sieciowymi , w związku z tym zamawiający nie dokonał podziału zamówienia na części. Dzielenie zamówienia na części pod kątem ilości w efekcie przyniosłoby wzrost cen w stosunku do całkowitego zakresu zamówienia, ze względu na konieczność odrębnego wliczania kosztów pośrednich przez każdego ze startujących wykonawców (np. koszty ubezpieczenia, transportu, koordynatorów, systemu utrzymania gwarancji). Niniejsze zamówienie dotyczy zakresu o zasięgu, który sprawia, iż wykonanie go w ramach jednej części i przez jednego wykonawcę będzie stanowić najbardziej efektywny z punktu widzenia technicznego i formalnego sposób realizacji. Zamawiający otrzyma również gwarancję na dostarczony przedmiot zamówienia od jednego wykonawcy, a w przypadku większej liczby wykonawców mogłyby wystąpić duże problemy z wyegzekwowaniem roszczeń. Zastosowany ewentualnie podział zamówienia na części nie zwiększyłby konkurencyjności w sektorze małych i średnich przedsiębiorstw – zakres zamówienia jest zakresem typowym, umożliwiającym złożenie oferty wykonawcom z grupy małych lub średnich przedsiębiorstw. Zgodnie z treścią motywu 78 dyrektywy, Instytucja zamawiająca powinna mieć obowiązek rozważenia celowości podziału zamówień na części, jednocześnie zachowując swobodę autonomicznego podejmowania decyzji na każdej podstawie, jaką uzna za stosowną, nie podlegając nadzorowi administracyjnemu ani sądowemu.

Reasumując, zamawiający nie dokonał podziału zamówienia na części ze względu na to, że podział taki groziłby nadmiernymi trudnościami technicznymi oraz nadmiernymi kosztami wykonania zamówienia. Niedokonanie podziału zamówienia podyktowane było zatem względami ekonomicznymi, technicznymi, organizacyjnym oraz charakterem przedmiotu zamówienia.

Ponadto, istnieje ryzyko, że w przypadku podzielenia zamówienia na części, na którąś z nich mogłaby nie zostać złożona żadna oferta wykonawcy, co skutkowałoby tym, iż dany zakres mógłby nie zostać zrealizowany.

Zamawiający nie przewiduje udzielania zamówień, o których mowa w art. 214 ust. 1 pkt 8.

# V 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.

1. Zastrzeżenie informacji może dotyczyć nie tylko oferty, ale i innych dokumentów czy informacji składanych przez wykonawcę w postępowaniu. Dla skuteczności dokonanego zastrzeżenia należy wypełnić następujące warunki:

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

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

# VI Wymagania dotyczące wadium

W postępowaniu nie wymaga się wadium.

# VII Opis przedmiotu zamówienia

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

1. **NAS I – 1 szt.:**

|  |  |  |
| --- | --- | --- |
| 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 | |
| Dodatkowe akcesoria | | Przesuwny zestaw szyn rack |
| Konserwacja | | Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack |
| Gwarancja | | Wykonawca udzieli gwarancji:   * 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack |

1. **NAS II – 1 szt.:**

|  |  |  |
| --- | --- | --- |
| Minimalne wymagania Zamawiającego | | |
| Typ urządzenia | Serwer NAS | |
| Obudowa | Rack | |
| Procesor | Czterordzeniowy procesor o taktowaniu 3,35 GHz (z przyspieszeniem do 3.6 GHz) | |
| Sprzętowy mechanizm szyfrowania | Tak (AES-NI) | |
| Pamięć  RAM | min. 8 GB pamięci ECC UDIMM  z możliwością rozszerzenia do min. 32 GB | |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 24 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń Infiniband | |
| Porty zewnętrzne | Minimum:   * 2 porty USB 3.2.1 * 1 gniazdo rozszerzenia | |
| Porty sieciowe | Minimum:   * 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) * 1 port 10GbE RJ45 * Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8 | |
| Funkcja Wake on LAN/WAN | Tak | |
| Gniazdo rozszerzeń PCIe 3.0 | Min. 1x 4-liniowe gniazdo x8 Gen. 3 | |
| Wentylator obudowy | Min. 3 wentylatory 60 mm x 60 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: * 200 TB (wymagana pamięć 32 GB) * 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 SMB/NFS/AFP/FTP: 2 000 | |
| Uprawnienia | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) | |
| Wirtualizacja | Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack® | |
| Usługa katalogowa | Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń. | |
| Bezpieczeństwo | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne  blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) | |
| Obsługiwane przeglądarki | Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 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 udostępnionych * 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 | Wykonawca udzieli gwarancji:   * 3 lata na urządzenie główne * 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack | |
| Dodatkowe akcesoria | | Przesuwny zestaw szyn rack |
| Konserwacja | | Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack |
| Gwarancja | | Wykonawca udzieli gwarancji:   * 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack |

1. **Dyski twarde do NAS – 14 szt.**

|  |  |
| --- | --- |
| 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. |

1. **Zarządzane urządzenia sieciowe z obsługą VLAN – 2 szt.:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Minimalne wymagania Zamawiającego** | |
|  | **CECHY ZARZĄDZANIA** | |
|  | Typ przełącznika | Zarządzany |
|  | Przełącznik wielowarstwowy | L2/L3 |
|  | Obsługa jakość serwisu (QoS) | Tak |
|  | Zarządzany w chmurze | Tak |
|  | Zarządzanie przez stronę www | Tak |
|  | Inspekcja ARP | Tak |
|  | Konfigurowanie ustawień lokalizacji (CLI) | Tak |
|  | Obsługa MIB | Tak |
|  | **OCHRONA** | |
|  | Funkcje DHCP | DHCP relay, DHCP server, DHCPv6 client |
|  | Lista kontrolna dostępu (ACL) | Tak |
|  | Zasady Listy Kontroli Dostępu (ACL) | 1024 |
|  | IGMP snooping | Tak |
|  | Ochrona hasłem | Tak |
|  | obsługuje SSH/SSL | Tak |
|  | Filtrowanie adresów MAC | Tak |
|  | Szyfrowanie / bezpieczeństwo | HTTPS, SSH, SSL/TLS |
|  | **PORTY I INTERFEJSY** | |
|  | Podstawowe przełączanie RJ-45 Liczba portów Ethernet | 48 |
|  | Podstawowe przełączania Ethernet RJ-45 porty typ | Gigabit Ethernet (10/100/1000) |
|  | Ilość slotów Modułu SFP+ | 4 |
|  | Liczba portów USB 2.0 | 1 |
|  | **SIEĆ** | |
|  | Standardy komunikacyjne | IEEE 802.1D, IEEE 802.1w, IEEE 802.1s, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad |
|  | Obsługa 10G | Tak |
|  | Dublowanie portów | Tak |
|  | Protokół drzewa rozpinającego | Tak |
|  | Blokowanie head-of-line (HOL) | Tak |
|  | Prędkość transferu danych przez Ethernet LAN | 10,100,1000 Mbit/s |
|  | Kontrola wzrostu natężenia ruchu | Tak |
|  | Automatyczne MDI/MDI-X | Tak |
|  | Podpora kontroli przepływu | Tak |
|  | Agregator połączenia | Tak |
|  | Obsługa sieci VLAN | Tak |
|  | Liczba VLANs | 4094 |
|  | **PRZESYŁANIE DANYCH** | |
|  | Wielkość tabeli adresów | 16000 wejścia |
|  | Zgodny z Jumbo Frames | Tak |
|  | Rozszerzenie Jumbo Frames | 9000 |
|  | **FUNKCJE MULTICAST** | |
|  | Obsługa Multicast | Tak |
|  | **PROTOKOŁY** | |
|  | Protokoły zarządzające | SNMP |
|  | **KONSTRUKCJA** | |
|  | Możliwości montowania w stelażu | Tak |
|  | Przycisk reset | Tak |
|  | Diody LED | Tak |
|  | **WYDAJNOŚĆ** | |
|  | Procesor wbudowany | Tak |
|  | Taktowanie procesora | 800 MHz |
|  | Pojemność pamięci wewnętrznej | 512 MB |
|  | Wielkość pamięci flash | 256 MB |
|  | Aktualizacje oprogramowania urządzenia | Tak |
|  | **MOC** | |
|  | Zasilacz dołączony | Tak |
|  | **WARUNKI PRACY** | |
|  | Zakres temperatur (eksploatacja) | -5 - 50 °C |
|  | Zakres temperatur (przechowywanie) | -25 - 70 °C |
|  | Zakres wilgotności względnej | 10 - 90% |
|  | Dopuszczalna wilgotność względna | 10 - 90% |

1. **UTM – 2 sztuki**

**Wymagania Ogólne**

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

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

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

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

**Redundancja, monitoring i wykrywanie awarii**

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

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 5 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

**Funkcje Systemu Bezpieczeństwa:**

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

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

**Polityki, Firewall**

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

**Połączenia VPN**

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem  128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman  grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* Pracę w trybie Portal  - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

**Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

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

**Funkcje SD-WAN**

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

**Zarządzanie pasmem**

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

**Ochrona przed malware**

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

**Ochrona przed atakami**

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

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

**Kontrola WWW**

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

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

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

**Logowanie**

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

**Testy wydajnościowe oraz funkcjonalne**

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

**Serwisy i licencje**

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

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.

**Gwarancja oraz wsparcie**

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

**Opisy do wymagań ogólnych**

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

**6. Licencje UTM – 2 sztuki**

**Serwisy i licencje**

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje dla UTM z pkt. 5 Opisu przedmiotu zamówienia.

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum do końca trwania projektu tj. 30.06.2026r.

**7. Serwer – 2 sztuki**

|  |  |
| --- | --- |
| **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 |
| **Dyski twarde** | * Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **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](http://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 angi*e*lskim. * 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. |

**8. UPS – 1 sztuka.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa elementu, parametru lub cechy** | **Opis wymagań** |
| 1 | Moc pozorna | 3000VA |
| 2 | Moc rzeczywista | 3000W |
| 3 | Topologia (klasyfikacja IEC 62040-3) | Podwójna konwersja on-line z korekcją wejściowego współczynnika mocy systemu (PFC) |
| 4 | Sprawność przy pracy normalnej (100% obc.) | <94% |
| 5 | Sprawność w trybie podwyższonej sprawności (100% obc.) | >98% |
| 6 | Współczynnik mocy | 1 |
| 7 | Czas przełączenia na baterię | 0 ms |
| 8 | Możliwość pracy równoległej | tak |
| 9 | Liczba, typ gniazd wyjściowych | 8 gniazd IEC C13 (10A) + 2 gniazda IEC C19 (16A), w tym 2 zarządzalne grupy wraz z pomiarem zużytej energii |
| 10 | Typ gniazda wejściowego | 1 IEC C20 (16A) lub blok zacisków w wersji HotSwap MBP HW |
| 11 | Czas podtrzymania dla 100% obciążenia dla pf=1 | 3 min |
| 12 | Czas podtrzymania przy 50% obciążenia dla pf=1 | 10 min |
| 13 | Dodatkowe baterie | Możliwość dołożenia maksymalnie 4 zewnętrznych modułów bateryjnych |
| 14 | Napięcie znamionowe | 200/208/220/230/240 V |
| 15 | Tolerancja napięci prostownika | 176V – 276 V (100-276V przy <33% obciążeniu) |
| 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 | 9Ah 12V, minimum 6 szt. |
| 32 | Czas ładowania baterii do poziomu 90% | < 1,5 godz. do 90% pojemności użytkowej |
| 33 | Interfejs komunikacyjny | •  USB   • RS232 DB-9 żeński (HID)   • 1 blok mini-zacisków dla zdalnego załączania/wyłączania   • 1 blok mini-zacisków do zdalnego wyłączania   • 1 blok mini-zacisków przekaźnika wyjściowego |
| 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 : 4 LED |
| • 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) |
| • LED w trybie obejścia (kolor pomarańczowy) |
| 37 | Kolor | Czarny RAL 9005 |
| 38 | Typ obudowy | Uniwersalna Tower/Rack 2U |
| 39 | Wyposażenie standardowe | UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa, instrukcja szybkiego montażu |
| 1 x kabel szeregowy RS-232, |
| 1 x kabel komunikacyjny USB |
| 1 x kable wyjściowe IEC 16A |
| 2 x kable wyjściowe IEC 10A |
| uchwyty kablowe |
| 1 x zestaw szyn montażowych 19’ |
| podstawki do montażu wieżowego |
| 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 |
| 41 | Zgodność ze standardem Energy Star | Tak |
| 42 | Maksymalna szerokość | 440 mm |
| 43 | Maksymalna wysokość | 86,5 mm |
| 44 | Maksymalna głębokość | 605 mm |
| 45 | Maksymalny ciężar | 27,4 kg |
| 46 | Poziom hałasu w odl. 1m | <47 dBA dla pracy normalnej |
| 47 | Znaki bezpieczeństwa | CE, C-Tick, IEC/EN 62040-1, IEC/EN 62040-2: Kat. C1, IEC/EN 62040-3 |
| 48 | Gwarancja producenta | 2 lata |

1. **Licencje serwerowe – 2 sztuki**

Licencje systemu operacyjnego Microsoft Windows Server 2025 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 2025 Datacenter.

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2025 Datacenter, Zamawiający wymaga dostarczenia licencji dla 2 serwerów oraz instalacji i migracji obecnego środowiska. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:

1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2022.
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:
18. pozwalają na zmianę rozmiaru w czasie pracy systemu,
19. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
20. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
21. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
22. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
23. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
24. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
25. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
26. Możliwość wykorzystania standardu http/2.
27. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
28. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
29. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
30. Mechanizmy logowania w oparciu o: a) login i hasło,
31. karty z certyfikatami (smartcard),
32. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
33. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
34. określonych grup użytkowników,
35. zastosowanej klasyfikacji danych,
36. centralnych polityk dostępu w sieci,
37. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
38. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
39. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
40. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
41. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji    
    w dokumentach (Digital Rights Management).
42. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
43. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
44. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
45. 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.,

1. zdalna dystrybucja oprogramowania na stacje robocze,
2. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
3. 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.

1. szyfrowanie plików i folderów,
2. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
3. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
4. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
5. serwis udostępniania stron WWW,
6. wsparcie dla protokołu IP w wersji 6 (IPv6),
7. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
8. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
9. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
10. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover    
    z jednoczesnym zachowaniem pozostałej funkcjonalności.
11. 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.

1. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
2. wsparcie dla rozwiązania Kubernetes.
3. 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.
4. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
5. mechanizmy deduplikacji i kompresji na wolumenach.
6. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
7. mechanizm konfiguracji połączenia VPN do platformy Azure.
8. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
9. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
10. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).
11. **Licencje dostępowe – 40 sztuk**
12. Licencje dostępowe na użytkownika

* Wymagana licencja typu Cal User OEM do systemu Windows Server 2025 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.

1. Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2025 na użytkownika:

* Licencja dostępowa dla użytkownika umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2025 typu User Cal z wdrożoną rolą Active Directory

1. **Oprogramowanie do wykonywania kopii zapasowych – 5 licencji uniwersalnych.**

Licencja musi być na bezterminowa, bez żadnych dodatkowych opłat a wsparcie na minimum do końca trwania projektu tj. 30.06.2026r.

|  |  |
| --- | --- |
| **Lp.** | **Minimalne wymagania Zamawiającego** |
| 1. **Wymagania ogólne** | |
|  | 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, |
|  | 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 |
|  | 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. |
| 1. **Całkowite koszty posiadania** | |
|  | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
|  | Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków |
|  | Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. |
|  | Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. |
|  | Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. |
|  | Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach 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. |
|  | Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. |
|  | Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania |
|  | Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) |
|  | Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu |
|  | Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API |
|  | Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji |
|  | Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji |
|  | Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania |
|  | Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |
|  | Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej |
| 1. **Wymagania RPO** | |
|  | Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej |
|  | Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. |
|  | Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru |
|  | Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. |
|  | Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. |
|  | Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy. |
|  | Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |
|  | Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. |
|  | 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. |
|  | Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |
|  | Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. |
|  | Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. |
|  | Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |
|  | Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
|  | Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| 1. **Wymagania RTO** | |
|  | Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. |
|  | Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
|  | Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami |
|  | Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre |
|  | Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. |
|  | Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków |
|  | Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. |
|  | Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików |
|  | Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. |
|  | Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell |
|  | Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM |
|  | Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI |
|  | Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| 1. **Ograniczenie ryzyka** | |
|  | Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
|  | Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. |
|  | Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem |
|  | Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. |
|  | Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| 1. **Środowiska fizyczne** | |
|  | Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego |
|  | Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych |
|  | Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE |
|  | Rozwiązanie musi wspierać system operacyjny macOS |
|  | Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix |
|  | Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) |
|  | Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster |
|  | Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów |
|  | Rozwiązanie musi wspierać backup podłączonych dysków USB |
|  | Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym |
|  | Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) |
|  | Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone |
|  | Rozwiązanie musi wspierać kontrolę pasma sieciowego |
|  | Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych |
|  | Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN |
|  | Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft |
|  | Rozwiązanie musi wspierać technologię BitLocker |
|  | Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania |
|  | Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej 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 |
|  | Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych |
|  | Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu. |
|  | 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 |
|  | Rozwiązanie musi wspierać szyfrowanie |
|  | Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne |
|  | Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego |
|  | Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej |
|  | Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |
| 1. **Monitoring** | |
|  | System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich |
|  | System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
|  | System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
|  | System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter |
|  | System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn |
|  | System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel |
|  | System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk |
|  | System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora |
|  | System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów |
|  | System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) |
|  | System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna |
|  | System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego |
|  | System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta |
|  | System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. |
|  | System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. |
|  | System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
|  | System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4 |
| 1. **Raportowanie** | |
|  | System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
|  | System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
|  | System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. |
|  | System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V |
|  | System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF |
|  | System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc |
|  | System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach |
|  | System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów |
|  | System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych |
|  | System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych |
|  | System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury |
|  | System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta |
|  | System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. |
|  | System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. |
|  | System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
|  | System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) |
|  | System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |

**12. Oprogramowanie Antywirusowe – 40 licencji**

Przedmiotem zamówienia jest odnowienie Licencji antywirusowej ESET PROTECT Advanced ON-PREM, o identyfikatorze publicznym licencji: 3A6-P27-N2D, Zamawiającego w ilości sztuk 36 oraz zakup 4 nowych licencji. Zamawiający przyjmie rozwiązanie równoważne do obecnie posiadanej licencji o parametrach oraz funkcjonalnościach, minimalnych opisanych w OPZ.

Zamawiający wymaga aby licencja była minimalnie na okres do 30.06.2026 roku.

Administracja zdalna

1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu [WWW.](http://WWW/)
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:
   1. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
   2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
   3. Buforowanie ruchu HTTPS.
6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
   1. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
      1. Google Authenticator,
      2. Microsoft Authenticator,
      3. Authy,
      4. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
8. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
   1. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej:
      1. adresy sieciowe IP,
      2. aktywne zagrożenia,
      3. stan funkcjonowania oraz ochrony,
      4. wersja systemu operacyjnego,
      5. podzespoły komputera.
10. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
    1. wyrażenie CRON,
    2. codziennie,
    3. cotygodniowo,
    4. co miesiąc,
    5. co rok,
    6. po wystąpieniu nowego zdarzenia,
    7. po automatycznym umieszczeniu hosta w grupie dynamicznej.
11. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim
    1. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania
12. Rozwiązanie musi mieć możliwość tagowania obiektów.
13. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
    1. Eksport danych musi być możliwy w co najmniej następujących formatach:
       1. JSON,
       2. LEEF,
       3. CEF.

Ochrona stacji roboczych - Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   1. wirus,
   2. trojan,
   3. robak,
   4. adware,
   5. spyware,
   6. dialer,
   7. phishing,
   8. backdoor.
4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
   1. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
   2. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
   3. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    1. całego dysku,
    2. wybranych katalogów,
    3. pojedynczych plików,
    4. plików spakowanych oraz skompresowanych,
    5. dysków sieciowych,
    6. dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    1. wybranych plików,
    2. wybranych procesów,
    3. wybranych lokalizacji,
    4. wybranych rozszerzeń,
    5. nazwy wykrycia,
    6. sumy kontrolnej (SHA1).
12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
    2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
    3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
14. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
    1. typ urządzenia:
       1. pamięci masowe,
       2. optyczne pamięci masowe,
       3. pamięci masowe Firewire,
       4. urządzenia do tworzenia obrazów,
       5. drukarki USB,
       6. urządzenia Bluetooth,
       7. czytniki kart inteligentnych,
       8. modemy,
       9. porty LPT/COM,
       10. urządzenia przenośne.
    2. parametry urządzenia:
       1. numer seryjny,
       2. producent,
       3. model.
    3. typ dostępu:
       1. brak możliwości zapisu,
       2. pełen dostęp,
       3. ostrzeżenie użytkownika,
       4. brak dostępu.
18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i

wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

* 1. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  2. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  3. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i

użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

* 1. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
   1. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów

filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

* 1. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
  2. Raport musi posiadać co najmniej:
     1. Listę zainstalowanych aplikacji,
     2. Listę usług systemowych,
     3. Informacje o systemie operacyjnym i sprzęcie,
     4. Listę aktywnych procesów i połączeń sieciowych,
     5. Harmonogram systemu operacyjnego,
     6. Szczegóły pliku hosts,
     7. Informacje o sterownikach.

1. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
   1. antywirus,
   2. zapora osobista
   3. sandbox,
   4. antyspyware,
   5. metody heurystyczne.
2. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
3. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
   1. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
   2. Ochrona musi być realizowana w oparciu o co najmniej:
      1. globalna czarna lista RBL,
      2. czarna lista użytkownika,
      3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
4. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
   1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
      1. Skanowanie portów TCP oraz UDP,
      2. Wykrywanie duplikacji adresu IP,
      3. Atak zatruwania ARP,
      4. Nieprawidłowa długość pakietu TCP oraz UDP.
   2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
      1. RDP,
      2. SMB,
      3. My SQL,
      4. MS SQL.
   3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
5. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
   1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
   2. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
      1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
      2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
      3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
      4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
         1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
6. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
   1. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
   2. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
   3. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja

TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.

1. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.
   1. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
   2. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:
      1. Treść komunikatu,
      2. Obraz.

Ochrona stacji roboczych – MacOS

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   1. wirus,
   2. trojan,
   3. robak,
   4. adware,
   5. spyware,
   6. dialer,
   7. phishing,
   8. backdoor.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość

wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

1. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
2. Rozwiązanie musi chronić pliki co najmniej za pomocą:
   1. Sygnatur wirusów.
   2. Reputacji chmurowej.
3. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
4. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
   2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
5. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   1. całego dysku,
   2. wybranych katalogów,
   3. pojedynczych plików,
   4. plików spakowanych oraz skompresowanych,
   5. Dysków sieciowych,
   6. dysków przenośnych.
6. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   1. wybranych plików,
   2. wybranych procesów,
   3. wybranych lokalizacji,
   4. wybranych rozszerzeń,
   5. nazwy wykrycia,
   6. sumy kontrolnej (SHA1).
7. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
   1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.
   2. Zapora osobista musi posiadać co najmniej dwa tryby pracy:
      1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
      2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

Ochrona stacji roboczych – Linux

1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:
   1. Ubuntu Desktop,
   2. Red Hat Enterprise Linux
   3. Linux Mint.
2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:
   1. Cinnamon,
   2. GNOME,
   3. KDE,
   4. MATE,
   5. XFCE.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   1. wirus,
   2. trojan,
   3. robak,
   4. adware,
   5. spyware,
   6. dialer,
   7. phishing,
   8. backdoor.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość

wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

1. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
2. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
3. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   1. całego dysku,
   2. wybranych katalogów,
   3. pojedynczych plików,
   4. plików spakowanych oraz skompresowanych,
   5. dysków sieciowych,
   6. dysków przenośnych.
4. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   1. wybranych plików,
   2. wybranych procesów,
   3. wybranych lokalizacji,
   4. wybranych rozszerzeń,
5. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
   1. typ urządzenia:
      1. pamięci masowe,
      2. optyczne pamięci masowe,
   2. parametry urządzenia:
      1. numer seryjny,
      2. producent,
      3. model.
   3. typ dostępu:
      1. brak możliwości zapisu,
      2. pełen dostęp,
      3. brak dostępu.

Ochrona serwera – Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
   1. Microsoft Windows Server 2012 R2,
   2. Microsoft Windows Server 2016,
   3. Microsoft Windows Server 2019,
   4. Microsoft Windows Server 2022,
   5. Microsoft Windows Server 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   1. wirus,
   2. trojan,
   3. robak,
   4. adware,
   5. spyware,
   6. dialer,
   7. phishing,
   8. backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
   2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   1. całego dysku,
   2. wybranych katalogów,
   3. pojedynczych plików,
   4. plików spakowanych oraz skompresowanych,
   5. dysków sieciowych,
   6. dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    1. wybranych plików,
    2. wybranych procesów,
    3. wybranych lokalizacji,
    4. wybranych rozszerzeń,
    5. nazwy wykrycia,
    6. sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i

wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

* 1. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  2. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  3. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i

użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

* 1. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
   1. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów

filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

* 1. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
  2. Raport musi posiadać co najmniej:
     1. Listę zainstalowanych aplikacji,
     2. Listę usług systemowych,
     3. informacje o systemie operacyjnym i sprzęcie,
     4. Listę aktywnych procesów i połączeń sieciowych,
     5. harmonogram systemu operacyjnego,
     6. Szczegóły pliku hosts,
     7. Informacje o sterowników.

1. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
   1. antywirus,
   2. zapora osobista
   3. sandbox,
   4. antyspyware,
   5. metody heurystyczne.
2. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
3. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
4. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
   1. typ urządzenia:
      1. pamięci masowe,
      2. optyczne pamięci masowe,
      3. pamięci masowe Firewire,
      4. urządzenia do tworzenia obrazów,
      5. drukarki USB,
      6. urządzenia Bluetooth,
      7. czytniki kart inteligentnych,
      8. modemy,
      9. porty LPT/COM,
      10. urządzenia przenośne.
   2. parametry urządzenia:
      1. numer seryjny,
      2. producent,
      3. model.
   3. typ dostępu:
      1. brak możliwości zapisu,
      2. pełen dostęp,
      3. ostrzeżenie użytkownika,
      4. brak dostępu.
5. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
   1. MS SQL,
   2. Active Directory,
   3. IIS,
   4. Sysvol,
   5. DNS,
   6. DHCP,
   7. Hyper-V,
   8. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
6. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
   1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
      1. Skanowanie portów TCP oraz UDP,
      2. Wykrywanie duplikacji adresu IP,
      3. Atak zatruwania ARP,
      4. Nieprawidłowa długość pakietu TCP oraz UDP.
   2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
      1. RDP,
      2. SMB,
      3. My SQL,
      4. MS SQL.
   3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
7. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
8. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
   1. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
      1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
      2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
      3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
      4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
         1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

Ochrona serwera – Linux

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
   1. RedHat Enterprise Linux (RHEL),
   2. Rocky Linux,
   3. Ubuntu,
   4. Debian,
   5. SUSE Linux Enterprise Server (SLES),
   6. Oracle Linux,
   7. Amazon Linux.
2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   1. wirus,
   2. trojan,
   3. robak,
   4. adware,
   5. spyware,
   6. dialer,
   7. phishing,
   8. backdoor.
3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   1. całego dysku,
   2. wybranych katalogów,
   3. pojedynczych plików,
   4. plików spakowanych oraz skompresowanych,
   5. dysków sieciowych,
   6. dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   1. wybranych plików,
   2. wybranych procesów,
   3. wybranych lokalizacji,
   4. wybranych rozszerzeń,
10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
    1. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
12. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
    1. proces budowania obrazu kontenera,
    2. wdrażanie obrazu kontenera.

Mobile Device Management

1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
   1. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:
      1. Android,
      2. iOS,
      3. iPadOS.
   2. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
      1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
      2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
      3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
      4. Apple Business Manager (ABM),
      5. Android Enterprise (co najmniej w zakresie Device Owner).
3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   1. usunięcie zawartości urządzenia,
   2. przywrócenie urządzenia do ustawień fabrycznych,
   3. zablokowanie urządzenia,
   4. uruchomienie sygnału dźwiękowego,
   5. lokalizację GPS,
   6. Resetowanie hasła blokady ekranu.
4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
5. MDM musi umożliwiać co najmniej:
   1. Dla systemów iOS oraz iPadOS
      1. konfigurację kont e-mail,
      2. konfigurację połączeń VPN,
      3. Konfigurację połączeń Wi-Fi,
      4. Konfigurację listy certyfikatów,
      5. możliwość uruchomienia trybu jednej aplikacji.
   2. Dla systemu Android:
      1. blokadę wykonywania połączeń,
      2. blokadę konfiguracji sieci Wi-Fi,
      3. blokadę konfiguracji tuneli VPN,
      4. zarządzenie aktualizacjami sytemu operacyjnego,
      5. blokadę zmiany tapety urządzenia.

Mobile Threat Defense (MTD) dla systemu Android

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
   1. Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
   2. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:
   1. Złożoność kodu blokady ekranu:
      1. Wzór,
      2. PIN,
      3. Hasło,
   2. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,
   3. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.
5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   1. nazwę aplikacji,
   2. nazwę pakietu,
   3. kategorię sklepu Google Play,
   4. uprawnienia aplikacji,
   5. pochodzenie aplikacji z nieznanego źródła.
6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

Sandbox w chmurze

1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi wspierać systemy w tym co najmniej:
   1. Microsoft Windows 10 oraz 11,
   2. Microsoft Windows Server,
   3. macOS 11 (Big Sur) oraz nowszych
   4. RedHat Enterprise Linux (RHEL),
   5. Rocky Linux,
   6. Ubuntu,
   7. Debian,
   8. SUSE Linux Enterprise Server (SLES),
   9. Oracle Linux,
   10. Amazon Linux.
4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
   1. archiwa,
   2. skrypty,
   3. pliki wykonywalne,
   4. pliki rejestru systemowego (.reg),
   5. możliwy spam,
   6. dokumenty.
7. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
   1. natychmiast po ich przeanalizowaniu,
   2. po upływie 30 dni,
   3. nigdy.
8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
12. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
    1. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
    1. czysty,
    2. podejrzany,
    3. bardzo podejrzany,
    4. szkodliwy.
14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:
    1. wstrzymania uruchamiania pobieranych plików z następujących źródeł:
       1. przeglądarki internetowe,
       2. programy poczty e-mail,
       3. nośniki wymienne,
       4. pliki wyodrębnione z archiwum.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.

Szyfrowanie

1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
5. Rozwiązanie musi posiadać autentykacje typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
   1. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
   2. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
   1. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
   2. Hasło odzyskiwania nie może być krótsze niż 8 znaków.
   3. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
10. Rozwiązanie musi wspierać dyski wykorzystującego funkcji OPAL w wersji co najmniej 2.0.
11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.

**13. Wsparcie lokalne przy wdrożeniu zakupionego sprzętu komputerowego – 1 dzień roboczy**

W ramach wsparcia lokalnego przewiduje się realizację prac wdrożeniowych związanych z podłączeniem sprzętu informatycznego na warstwie fizycznej oraz instalacją oprogramowania. Prace te będą prowadzone w trybie hybrydowym – częściowo w siedzibie Zamawiającego, a częściowo zdalnie, przy wykorzystaniu połączenia z systemami Zamawiającego.

Wsparcie lokalne dotyczy wyłącznie czynności realizowanych na warstwie fizycznej, w szczególności podłączenia, montażu i uruchomienia sprzętu, i powinno być zapewnione przez minimum 1 dzień roboczy lub do momentu zakończenia podłączania całego sprzętu dostarczonego w ramach zamówienia – w zależności od tego, które z tych zdarzeń nastąpi wcześniej.

# VIII Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV)

**CPV 48820000-2 serwery**

**CPV 48000000-8 pakiety oprogramowania i systemy informatyczne**

**CPV 72268000-1 usługi dostawy oprogramowania**

# IX Miejsce i Terminy wykonania zamówienia

Zamówienie będzie wykonane w miejscu siedziby zamawiającego.

Zamówienie zostanie zrealizowane w ciągu **30 dni roboczych** od dnia podpisania umowy.

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

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

# X Warunki udziału w postępowaniu

1. udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki udziału w postępowaniu dotyczące:
2. zdolności do występowania w obrocie gospodarczym; Zamawiający nie określa warunku w ww. zakresie.
3. uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów; Zamawiający nie określa warunku w ww. zakresie.
4. sytuacji ekonomicznej lub finansowej; Zamawiający nie określa warunku w ww. zakresie
5. zdolności technicznej lub zawodowej w zakresie: Opis sposobu dokonywania oceny spełniania tego warunku:

**Do przedmiotu zamówienia :**

**Na potwierdzenie spełnienia warunku udziału w postępowaniu, dotyczącego zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca wykazał się odpowiednim doświadczeniem, tj. w ciągu ostatnich 3 lat przed upływem terminu składania ofert, w tym okresie realizuje, bądź zrealizował należycie co najmniej jedno zamówienie, które obejmowało swoim zakresem dostawę sprzętu komputerowego i/lub sprzętu komputerowego z oprogramowaniem na kwotę co najmniej 100 000,00 złotych brutto.**

1. 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.
2. 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.
3. Zamawiający wskazuje, że w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia lub w przypadku korzystania z podmiotów udostępniających zasoby na podstawie art. 118 ustawy Pzp Wykonawca lub minimum jeden Wykonawca wspólnie ubiegający się o zamówienie lub minimum jeden podmiot udostępniający zasoby musi posiadać pełne doświadczenie wskazane w warunku udziału w postępowaniu wskazane SWZ - dotyczy to konieczności wykazania doświadczenia wynikającego z powtarzalności wykonanych zamówień, tj. wykonania minimum 2 zamówień przez jeden podmiot.
4. Zamawiający może, oceniając zdolność techniczną lub zawodową, na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez Wykonawcę sprzecznych interesów, w szczególności zaangażowanie zasobów technicznych lub zawodowych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy może mieć negatywny wpływ na realizację zamówienia na każdym etapie postępowania (art. 116 ust. 2 ustawy Pzp).

# XI Przesłanki wykluczenia Wykonawcy

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

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

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

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

c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz.U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust.1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz.U. z 2021 r. poz. 523, 1292, 1559 i 2054),

d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,

e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,

f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),

g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,

h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej - lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;

3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

1. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
2. 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.
3. 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.
4. Zamawiający nie wprowadza w tym postępowaniu dodatkowych podstaw wykluczenia wskazanych w art. 109 ustawy Pzp.
5. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy Pzp.
6. 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.
7. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia zgodnie z art. 110 ust. 1 ustawy Pzp.
8. 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.
9. wykonawcy wymienieni w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.) albo wpisani na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, na podstawie decyzji w sprawie wpisu na ww. listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 powołanej ustawy;
10. wykonawcy, których 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 ze zm.) jest osoba wymieniona w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.) albo wpisani na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, lub będący takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile zostali wpisani na ww. listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w 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;
11. wykonawcy, których jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 ze zm.) jest podmiot wymieniony w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.) albo wpisany na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na ww. listę rozstrzygającej o zastosowaniu środka, o którym mowa w 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.
12. Wykluczenie, o którym mowa w ust. 1 następuje na okres trwania ww. okoliczności.

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

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

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

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

* Wykaz dostaw wykonanych w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - tj.w tym okresie, wraz z podaniem ich wartości, dat wykonania i podmiotów na rzecz, których usługi zostały wykonane, przed upływem terminu składania ofert w co najmniej jednym zamówieniu polegającym na dostawie sprzętu komputerowego i/lub dostawie sprzętu komputerowego z oprogramowaniem na kwotę co najmniej **100 000,00 złotych brutto wraz z dowodem należytego ich wykonania (na przykład w postaci referencji lub innych dokumentów) wg załącznika nr 8 do SWZ**
* oświadczenia Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2024 r. poz. 594), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej – **wg załącznika nr 4 do SWZ**

• Ponadto Zamawiający wymaga, aby Wykonawca wraz z ofertą złożył przedmiotowe środki dowodowe:

W odniesieniu do serwera (pkt. 7 OPZ)

a) 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.

b) 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.

c) Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

d) Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku

2. W odniesieniu do pozostałych przedmiotowych środków dowodowych zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane dostawy spełniają określone przez zamawiającego wymagania, cechy i kryteria.

3. 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.

4.Postanowień ust. 4 SWZ nie stosuje się:

1. w części w jakiej przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub,
2. pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.

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

# XIV Podwykonawcy

1. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z wnioskiem o dopuszczenie do udziału w postępowaniu albo odpowiednio wraz z ofertą, zobowiązanie podmiotu trzeciego do oddania do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów zg z załącznikiem nr 7.

6. Zobowiązanie podmiotu udostępniającego zasoby potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:

* zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
* sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
* czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje dostawy lub usługi, których wskazane zdolności dotyczą.

7. Podwykonawcy obowiązani są do złożenia wszelkich oświadczeń, w szczególności oświadczeń sankcyjnych i o braku przesłanek wykluczenia w takim zakresie w jakim dotyczą one Wykonawcy.

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

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
4. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
5. Zobowiązanie podmiotu udostępniającego zasoby lub inny środek dowodowy, o którym mowa w pkt 9.4 SWZ potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
6. 1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
7. 2) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
8. 3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.
9. Zamawiający oceni, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu a także zbada, czy nie zachodzą, wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
10. Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą, wobec tego podmiotu podstawy wykluczenia, Zamawiający zażąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
11. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia oświadczenia podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.
12. Wykonawcy wspólnie ubiegający się o realizację zamówienia
13. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku, Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
14. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia:

1)oświadczenia o których mowa w SWZ składa z ofertą każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenia te  potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu lub kryteriów selekcji w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu lub kryteriów selekcji.

2)w przypadku, gdy Wykonawcy wspólnie ubiegają się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni Wykonawcy. Oświadczenie należy złożyć wg wymogów załącznika nr 9 do SWZ. Oświadczenie to jest podmiotowym środkiem dowodowym.

3)zobowiązani są oni na wezwanie Zamawiającego, złożyć podmiotowe środki dowodowe, których mowa w SWZ, przy czym podmiotowe środki dowodowe składa odpowiednio Wykonawca/Wykonawcy, który/którzy wykazuje/-ą spełnienie warunku.

Jeżeli została 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.

# XVI Kryterium równoważności

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

# XVII Opis sposobu składania ofert w postępowaniu

1. Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej
2. W postępowaniu o udzielenie zamówienia publicznego komunikacja między Zamawiającym a wykonawcami odbywa się przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem <https://ezamowienia.gov.pl>.
3. Korzystanie z platformy e – Zamówienia jest bezpłatne.
4. **Ofertę wraz z oświadczeniami i dokumentami należy złożyć w terminie do dnia** **29.12.2025 do godz. 09:00**
5. **Otwarcie ofert nastąpi 29.12.2025 do godz. 10: 00**
6. Oferta powinna zawierać:
7. Formularz oferty **wg załącznika nr 1**;
8. Oświadczenie wstępne potwierdzające spełnienie warunków udziału w postępowaniu **wg załącznika nr 6;**
9. Oświadczenie o niepodleganiu wykluczeniu Wykonawcy z postępowania **wg załącznika nr 3**;
10. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu, zamieszcza informacje o tych podmiotach w oświadczeniu wg **załącznika nr 7 do SWZ**.
11. Pełnomocnictwo do reprezentowania Wykonawcy, w tym podpisania oferty, o ile prawo do podpisania oferty nie wynika z innych dokumentów złożonych wraz z ofertą. Treść pełnomocnictwa musi jednoznacznie określać czynności, co do wykonywania których pełnomocnik jest upoważniony;
12. Jeśli oferta zawiera tajemnicę przedsiębiorstwa, wyjaśnienia uzasadniające zastrzeżenie tajemnicy przedsiębiorstwa;
13. Wykonawca może przed upływem terminu składania ofert wycofać ofertę.

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

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

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

1. Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.
2. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.
3. Przy ocenie ofert w kryterium „Cena” (C) punkty zostaną przyznane w poniższy sposób:

* Cena – znaczenie 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.

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

# XIX Wzór umowy

1. Wzór Umowy stanowi Załącznik nr 2 do SWZ.

# XX 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”, Zamawiający informuje, że:

1) jest administratorem danych osobowych Wykonawcy oraz osób, których dane Wykonawca przekazał w niniejszym postępowaniu;

2) dane osobowe Wykonawcy przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego na zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd” w Gminie Pokój w ramach: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (DERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” prowadzonym w trybie podstawowym bez negocjacji;

3) odbiorcami danych osobowych Wykonawcy będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r., poz. 1320), dalej „ustawa Pzp”;

4) dane osobowe Wykonawcy będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, w sposób gwarantujący jego nienaruszalność.

5) obowiązek podania przez Wykonawcę danych osobowych bezpośrednio go dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

6) w odniesieniu do danych osobowych Wykonawcy decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;

7) Wykonawca posiada:

− na podstawie art. 15 RODO prawo dostępu do danych osobowych dotyczących Wykonawcy;

− na podstawie art. 16 RODO prawo do sprostowania danych osobowych, o ile ich zmiana nie skutkuje zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie narusza integralności protokołu oraz jego załączników;

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

− prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy Wykonawca uzna, że przetwarzanie jego danych osobowych narusza przepisy RODO;

8) Wykonawcy nie przysługuje:

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

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

− na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych Wykonawcy jest art. 6 ust. 1 lit. c RODO.

W przypadku, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 rozporządzenia 2016/679, wymagałoby niewspółmiernie dużego wysiłku, Zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu.

Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 rozporządzenia 2016/679, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego lub konkursu ani zmianą postanowień umowy w zakresie niezgodnym z ustawą.

Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania

o udzielenie zamówienia publicznego lub konkursu.

W przypadku danych osobowych zamieszczonych przez Zamawiającego w Biuletynie Zamówień Publicznych, prawa, o których mowa w art. 15 i art. 16 rozporządzenia 2016/679, są wykonywane w drodze żądania skierowanego do Zamawiającego.

# XXI Informacje Dodatkowe

Zamawiający w okresie 3 lat od dnia udzielenia zamówienia podstawowego, dotychczasowemu wykonawcy   
**nie przewiduje** udzielenia zamówienia polegającego na powtórzeniu podobnych usług.

Zamawiający **nie dopuszcza** składania ofert wariantowych.

Zamawiający **nie przewiduje** wymagań wskazanych w art. 96 ust. 2 pkt 2 ustawy Pzp.

Zamawiający **nie przewiduje** wymagań wskazanych w art. 94 ustawy Pzp.

Zamawiający **nie przewiduje** zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.

Zamawiający **nie wymaga** przeprowadzenia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy Pzp.

Zamawiający **nie przewiduje** rozliczenia między Zamawiającym a Wykonawcą w walutach obcych.

Zamawiający **nie przewiduje** zwrotu kosztów udziału w postępowaniu.

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

Zamawiający **nie przewiduje** zawarcia umowy ramowej

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

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

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

1. W postępowaniu o udzielenie zamówienia publicznego komunikacja między Zamawiającym, a Wykonawcami odbywa się przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem: https://ezamowienia.gov.pl

* Korzystanie z Platformy e-Zamówienia jest bezpłatne.
* Zamawiający wyznacza następującą osobę do kontaktu z Wykonawcami:

Hadamik Agnieszka, tel. +48 (77) 4693080, e-mail: zamowieniapubliczne@gminapokoj.pl

Tomasz Zimoch, tel. +48 (77) 4693080, e-mail: [zamowieniapubliczne@gminapokoj.pl](mailto:zamowieniapubliczne@gminapokoj.pl)

1. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego musi posiadać konto podmiotu „Wykonawca” na Platformie e-Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej https://ezamowienia.gov.pl/pl/regulamin/#regulamin-serwisu oraz informacje zamieszczone w zakładce „Centrum Pomocy”.
2. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie e-Zamówienia ani logowania do Platformy e-Zamówienia.
3. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe odwzorowania) musi być zgodny z wymaganiami określonymi w rozporządzeniu 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.
4. Dokumenty elektroniczne, o których mowa w § 2 ust. 1 rozporządzenia , o którym mowa w pkt 11.6 SWZ, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach rozporządzenia 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, z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki. W przypadku formatów, o których mowa w art. 66 ust. 1 ustawy Pzp, ww. regulacje nie będą miały bezpośredniego zastosowania.
5. Informacje, oświadczenia lub dokumenty, inne niż wymienione w § 2 ust. 1 rozporządzenia, o którym mowa w pkt 11.6 SWZ, przekazywane w postępowaniu sporządza się w postaci elektronicznej:

a) w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności z uwzględnieniem rodzaju przekazywanych danych (i przekazuje się jako załącznik),

lub

b) jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej (np. w treści wiadomości e-mail lub

w treści „Formularza do komunikacji”).

1. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstw w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t. j. Dz. U. z 2022 r., poz. 1233 ze zm.), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonymi odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”.

* Komunikacja w postępowaniu, z wyłączeniem składania ofert (sposób składania ofert opisano w rozdziale 13 SWZ) odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce „Formularze” („Formularze do komunikacji”). Za pośrednictwem „Formularzy do komunikacji” odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk „dodaj załącznik”).
* Możliwość korzystania w postępowaniu z „Formularzy do komunikacji” w pełnym zakresie wymaga posiadania konta „Wykonawcy” na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Do korzystania z „Formularzy do komunikacji” służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie e-Zamówienia.
* Wszystkie wysłane i odebrane w postępowaniu przez Wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce „Komunikacja”.
* Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji” wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
* Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa § 12 Regulamin Platformy e-Zamówienia,

a mianowicie:

* W celu prawidłowego korzystania z usług Platformy e-Zamówienia wymagany jest:

a) Komputer PC:

b) parametry minimum: Intel Core2 Duo, 2 GB RAM, HD,

c) zainstalowany jedne z poniższych systemów operacyjnych: MS Windows 7 lub nowszy, OSX/Mac OS 10.10, Ubuntu 14.04,

a) zainstalowana jedna z poniższych przeglądarek: Chrome 66.0 lub nowsza, Firefox 59.0 lub nowszy, Safari 11.1 lub nowsza, Edge 14.0 i nowsze,

albo

b)Tablet/Telefon:

c) parametry minimum: 4 rdzenie procesora, 2GB RAM, Android 6.0 Marshmallow, iOS 10.3,

d) przeglądarka Chrome 61 lub nowa

* Dla skorzystania z pełnej funkcjonalności może być konieczne włączenie w przeglądarce obsługi protokołu bezpiecznej transmisji danych SSL,

obsługi Java Script oraz cookies;

* Specyfikacja połączenia, formatu przesyłanych danych oraz kodowania

i oznaczania czasu odbioru danych:

a) specyfikacja połączenia – formularze udostępnione są za pomocą protokołu TLS 1.2,

b) format danych oraz kodowanie: formularze dostępne są w formacie HTML z kodowaniem UTF-8,

c) oznaczenia czasu odbioru danych: wszelkie operacje opierają się

o czas serwera i dane zapisywane są z dokładnością co do sekundy.

* W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia

technicznego dostępnego drogą elektroniczną poprzez formularz udostępniony na stronie internetowej https://ezamowienia.gov.pl w zakładce „Zgłoś problem”.

* W szczególnie uzasadnionych przypadkach uniemożliwiających komunikację Wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres e-mail: zamowieniapubliczne@gminapokoj.pl (nie dotyczy składania ofert w postępowaniu).

# XXIII 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), wartości podatku vat oraz wartości netto dla poszczególnych pozycji.
2. Cena oferty stanowi wynagrodzenie ryczałtowe.
3. Cena musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
4. Wykonawca poda w Formularzu Ofertowym stawkę podatku od towarów i usług (VAT) właściwą dla przedmiotu zamówienia, obowiązującą według stanu prawnego na dzień składania ofert. Określenie ceny ofertowej z zastosowaniem nieprawidłowej stawki podatku od towarów i usług (VAT) potraktowane będzie, jako błąd w obliczeniu ceny i spowoduje odrzucenie oferty,
5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
6. W przypadku rozbieżności pomiędzy ceną ryczałtową podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena ryczałtowa podana słownie.

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

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

# XXV Środki ochrony prawnej

1. Środki ochrony prawnej przewidziane są w dziale IX ustawy.
2. Środkami ochrony prawnej są odwołanie i skarga do sądu.
3. Środki ochrony prawnej przysługują wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 ustawy Pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
4. Odwołanie przysługuje na:
5. niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
6. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy;
7. zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.
8. 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.
9. Terminy wnoszenia odwołań.
10. Odwołanie wnosi się w terminie:
11. 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
12. 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 1.
13. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej.  
    Odwołanie w przypadkach innych niż określone w pkt 1 i 2 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest mniejsza niż progi unijne.
14. 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:
15. 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania
16. miesiąca od dnia zawarcia umowy, jeżeli zamawiający:  
    nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo
17. 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.
18. Odwołanie zawiera:
19. imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);
20. nazwę i siedzibę zamawiającego, numer telefonu oraz adres poczty elektronicznej zamawiającego;
21. 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;
22. 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;
23. określenie przedmiotu zamówienia;
24. wskazanie numeru ogłoszenia w przypadku zamieszczenia w Biuletynie Zamówień Publicznych albo publikacji w Dzienniku Urzędowym Unii Europejskiej;
25. 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;
26. zwięzłe przedstawienie zarzutów;
27. żądanie co do sposobu rozstrzygnięcia odwołania;
28. wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności;
29. podpis odwołującego albo jego przedstawiciela lub przedstawicieli;
30. wykaz załączników.
31. Do odwołania dołącza się:
32. dowód uiszczenia wpisu od odwołania w wymaganej wysokości;
33. dowód przekazania odpowiednio odwołania albo jego kopii zamawiającemu;
34. 3) dokument potwierdzający umocowanie do reprezentowania odwołującego.
35. Na orzeczenie Izby stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych.

# ZAŁĄCZNIKI

Załącznik nr 1 Formularz oferty

Załącznik nr 2 Istotne Postanowienia Umowy

Załącznik nr 3 Oświadczenie wykonawcy w zakresie niepodlegania wykluczeniu z postępowania

Załącznik nr 4 Oświadczenie o braku powiazań osobowych i kapitałowych

Załącznik nr 5 Oświadczenie Wykonawcy w zakresie Rodo

Załącznik nr 6 Wzór oświadczenia o spełnianiu warunków udziału w postępowaniu

Załącznik nr 7 Wzór zobowiązanie do oddania do dyspozycji niezbędnych zasobów

Załącznik nr 8 Wzór wykazu dostaw

Załącznik nr 9 Wzór oświadczenia Wykonawców wspólnie ubiegających się o udzielenie zamówienia