# Ogólny opis przedmiotu zamówienia i wymagań Zamawiającego

1. **Zakres przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa licencji, oprogramowania, fabrycznie nowego sprzętu komputerowego, wdrożenie systemów i rozwiązań teleinformatycznych, przeprowadzenie szkoleń oraz wykonanie diagnozy cyberbezpieczeństwa mających na celu podniesienie poziomu cyfryzacji urzędu w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego pn. „Dostawa sprzętu oraz oprogramowania w ramach projektu grantowego: Cyfrowa Gmina”o numerze **POPC.05.01.00-00-0001/21-00**

Szczegółowy zakres projektu składa się z następujących zadań:

1. **Dostawa stacji roboczych** - 5 szt.

Stacje robocze wraz z systemem operacyjnym będą wykorzystywane do realizacji usług publicznych, procedowania dokumentów, dla potrzeb aplikacji biurowych, obliczeniowych, w celu dostępu do Internetu oraz poczty elektronicznej.

1. **Dostawa licencji na pakiet oprogramowania biurowego** **(edytor tekstu, arkusz kalkulacyjny, narzędzie do przygotowania prezentacji)** - 5 szt.

Zbiór programów komputerowych służących do typowych zastosowań biurowych, takich jak edycja tekstu, wykonywanie obliczeń rachunkowo/księgowych, czy tworzenie i obsługa prezentacji, które mają zostać dostarczone jako jeden zintegrowany produkt.

1. **Dostawa szafy teleinformatycznej Rack 42U z wyposażeniem** – 1 kpl

Infrastruktura zostanie zainstalowana w nowej w pełni wyposażonej, profesjonalnej szafie teleinformatycznej typu Rack o wysokości 42U. Zakup szafy umożliwi zainstalowanie sprzętu w sposób profesjonalny, bezpieczny oraz zapewnieni dostęp jedynie dla osób uprawnionych.

1. **Dostawa zasilacza awaryjnego UPS Online (typ 1)** – 1 szt.

Zasilacz UPS Online umożliwi podtrzymanie pracy urządzeń serwerowych w przypadku wystąpienia awarii zasilania. Zasilacz (typ 1) zapewni podtrzymanie systemów informatycznych znajdujących się w szafie teleinformatycznej Rack

1. **Dostawa routera** – 1 szt.

Urządzenie służące do stworzenia własnej sieci lokalnej pełniące rolę węzła komunikacyjnego.

1. **Dostawa konsoli KVM** – 1 szt.

Konsola KVM ma umożliwić łatwe i szybkie zarządzanie kilkoma urządzeniami (np. serwerami) jednocześnie co znacznie przyśpieszy wykonywanie okresowych prac serwisowych. Konsola KVM zapewni dodatkowo integrację z istniejącymi elementami infrastruktury znajdującymi się w serwerowni.

1. **Dostawa serwerów (typ 1)** – 2 szt.

W celu zminimalizowania przestojów i zapewnienia nieprzerwanej pracy w przypadku awarii, Zamawiający zaplanował zakup dwóch serwerów, których zadaniem jest praca w kastrze wysokiej dostępności (ang. High Availability Cluster). Serwery w klastrze HA będą stanowić grupę urządzeń dublujących wzajemnie swoje funkcje, działając jak pojedynczy system. W przypadku awarii sprawny serwer przejmuje funkcje uszkodzonego, zapewniając ciągły czas pracy bez przestojów uzyskując, w ten sposób na poziomie sprzętowym niezawodność oraz wysokodostępność systemu.

Zakup fizycznych serwerów o wysokiej wydajności, uzupełnionych o macierz o której mowa w punkcie 8 oraz dedykowanych licencji oprogramowania, o których mowa w punkcie 11 umożliwi wdrożenie systemu wirtualizacji.

1. **Dostawa macierzy** – 1 szt.

Uzupełnieniem dla zakupu serwerów (typ 1) w klastrze HA będzie macierz, która umożliwi dostęp serwerów wirtualizacyjnych do współdzielonego bezpiecznego i szybkiego magazynu danych.

1. **Dostawa serwera do backupu** – 1 szt.

Bezpieczeństwo i ochronę danych w sieci lokalnej zapewni serwer backupu, dzięki któremu możliwe będzie wykonywanie bezpiecznych, integralnych kopii zapasowych. Backup będzie wykonywany dla danych z systemów dziedzinowych, maszyn wirtualnych oraz danych użytkowników.

Uzupełnieniem funkcjonalności serwera do backupu będzie zakup oprogramowania do backupu danych, o którym mowa w punkcie 12, które zautomatyzuje cały proces, zapewniając jego cykliczność i logowanie wykonanych zadań.

1. **Dostawa przełączników sieciowych zarządzalnych** – 2 szt.

W celu zapewnienia odpowiedniej szybkości transmisji danych oraz możliwości połączenia wszystkich elementów w jedną współpracującą ze sobą całość wymagana jest dostawa w pełni zarządzalnych przełączników sieciowych. Przełączniki zapewnią możliwość podziału sieci na odseparowane od siebie VLANy, co podniesie poziom bezpieczeństwa w sieci, zaś prędkości przełączników na poziomie 10Gb umożliwią zbudowanie rdzenia sieci o wysokiej wydajności co wpłynie na polepszenie skalowalności łączy, a w rezultacie prostszą i bardziej wydajną infrastrukturę sieciową.

1. **Dostawa licencji na system operacyjny, wirtualizację, licencji dostępowych** – 1 kpl

Dostawa licencji dla serwerów fizycznych (typ 1) na serwerowy system operacyjny w najnowszej wersji wraz z licencjami dostępowymi.

1. **Dostawa licencji na oprogramowanie do realizacji kopii zapasowych** – 1 kpl

Uzupełnieniem funkcjonalności serwera backupu będzie dostawa licencji oprogramowania do backupu danych, która zautomatyzuje cały proces zapewniając jego cykliczność i logowanie wykonanych zadań.

1. **Dostawa serwera (typ 2)** – 1 szt.

Zamawiający zaplanował zakup serwera wraz z systemem operacyjnym dla jednostki podległej.

1. **Dostawa zasilacza awaryjnego UPS Online (typ 2)** – 1 szt.

Zamawiający zaplanował zakup zasilacza awaryjnego dedykowanego dla serwera typ 2

1. **Usługi informatyczne z zakresu wdrożenia konserwacji i serwisu sprzętu informatycznego oraz oprogramowania**.

Celem prac jest przygotowanie do eksploatacji kompletnego środowiska teleinformatycznego, na potrzeby realizacji projektu, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. W ramach zadania wymagana jest wykonanie usługi instalacji, konfiguracji oraz uruchomienia urządzeń dostarczonych w ramach projektu oraz migracja na nowe rozwiązanie teleinformatyczne.

1. **Szkolenia stacjonarne dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania**.
2. **Szkolenia dla pracowników urzędu z cyberbezpieczeństwa**
3. **Dostawa specjalistycznego oprogramowania.**

W ramach projektu Zamawiający przewidział zakup narzędzia wspomagającego podniesienie bezpieczeństwa urzędu wobec współczesnych zagrożeń cybersecurity.

1. **Rozbudowa zabezpieczeń logicznych (firewall, IDS, IPS)**
Głównym elementem chroniącym dostęp do zasobów sieciowych będzie firewall sprzętowy. Zakup profesjonalnej zapory sieciowej zapewni ochronę przed cyberatakami z zewnątrz, zabezpieczy również lokalną sieć wraz z wszystkimi urządzeniami, które się w niej znajdują. Urządzenie to umożliwi filtrowanie oraz logowanie ruchu www, ochronę przed spamem, ochronę przed szkodliwym oprogramowaniem (np. malware, ransomware), a w przypadku konieczności pracy zdalnej zabezpieczy połączenie VPN, za pomocą którego realizowane będzie połączenie zdalne.
2. **Wykonanie diagnozy cyberbezpieczeństwa w Urzędzie.**
3. Usługa dotyczy przeprowadzenia diagnozy cyberbezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina".
4. **Ogólne wymagania Zamawiającego**

Niniejszy dokument ma celu umożliwienie dokonania wyboru najkorzystniejszej oferty na dostawy, usługi teleinformatyczne, szkolenia oraz realizację diagnozy cyberbezpieczeństwa, których podstawowym celem jest podniesienie poziomu cyfryzacji Urzędu oraz bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa). Dokument zawiera opis wymagań pod kątem kryteriów funkcjonalnych, technicznych i jakościowych oraz wskazuje technologie, które powinny być wykorzystane tak, aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania.

Opisane w dokumencie wymagania należy traktować jako **podstawowe i minimalne**, a te które zostały określone jako dodatkowe traktować należy jako nieobowiązkowe (fakultatywne).

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.

1. **Wymagania ogólne dotyczące sprzętu:**
2. Wszystkie dostarczone urządzenia muszą być fabrycznie nowe (wyprodukowane w roku 2022), bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wcześniejszych wystaw bądź prezentacji.
3. Dostarczone urządzenia muszą być wykonane w ramach bezpiecznych technologii oraz być wolne od obciążeń prawami osób trzecich, a także muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej.
4. Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt w miejsce wskazane przez Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta.
5. Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE oraz powinny posiadać certyfikację oraz oznaczenie CE.
6. Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów wyposażenia lub dodatkowych akcesoriów.
7. Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta.
8. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy urządzeń, w szczególności podzespoły montowane przez producenta były przez niego certyfikowane. Wykonawca nie będący producentem oferowanego sprzętu nie może samodzielnie dokonywać modyfikacji sprzętu i wprowadzać zmian w fabrycznej konfiguracji. Zamawiający nie dopuszcza dostawy urządzeń modyfikowanych przez sprzedawcę oraz nie dopuszcza modyfikacji na linii produkcyjnej dystrybutora.
9. **Wymagania ogólne dotyczące oprogramowania:**

Wykonawca zobowiązany jest dostarczyć Zamawiającemu:

1. drukowane certyfikaty licencyjne wystawione przez producenta oprogramowania, o ile nie są dostępne w formie elektronicznej;
2. nośniki instalacyjne oprogramowania, o ile nie są dostępne w formie elektronicznej;
3. adresy poczty elektronicznej, numery telefonów oraz inne dane dostępowe umożliwiające Zamawiającemu korzystanie ze wsparcia technicznego świadczonego przez producenta oprogramowania w pełnym zakresie, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
4. zestawienie dostarczonych Zamawiającemu pozycji w zakresie oprogramowania, zawierające m.in.: numer partii (SKU), pełna nazwa produktu, wersja i edycja oprogramowania, metryka licencyjna, rodzaj licencji (terminowa/bezterminowa), okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego,
5. standardowe warunki licencyjne producenta oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
6. standardowe warunki wsparcia technicznego producenta oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
7. oświadczenie producenta oprogramowania bądź autoryzowanego dystrybutora dostarczonego oprogramowania, potwierdzające dostawę licencji i objęcie ich wsparciem technicznym na poziomie zgodnym z wymaganiami Zamawiającego, o ile nie potwierdzają jej certyfikaty licencyjne i standardowe warunki wsparcia technicznego;
8. dostarczone oprogramowanie musi być opatrzone we wszystkie atrybuty oryginalności i legalności, wymagane przez producenta oprogramowania w zależności od dostarczanej wersji;
9. Zamawiający zastrzega sobie prawo do weryfikacji oprogramowania na etapie dostawy, również pod kątem jego legalności. W ramach procedury odbioru, Zamawiający zastrzega sobie prawo do przeprowadzenia weryfikacji legalności i oryginalności oprogramowania bezpośrednio u producenta oprogramowania, przed podpisaniem protokołu odbioru w sposób, który uzna za bezsporny. W przypadku wykrycia, że dostarczone w ramach umowy oprogramowanie nie jest nowe, było już używane lub było już wcześniej aktywowane Zamawiający odmówi przyjęcia oprogramowania (lub sprzętu z zainstalowanym oprogramowaniem) i wezwie Wykonawcę do usunięcia nieprawidłowości w wyznaczonym terminie.
10. **Wymagania ogólne dotyczące realizacji dostawy.**
11. Wykonawca na swój koszt i ryzyko dostarczy przedmiot zamówienia, zgodny z wymaganiami przedstawionymi w niniejszym dokumencie.
12. Wykonawca w cenie oferty uwzględni wszystkie koszty niezbędne do realizacji dostawy, m.in. rozładunek, wniesienie oraz utrzymanie porządku w czasie rozładunku prowadzonego na terenie urzędu.
13. Wykonawca, co najmniej na 3 dni przed dniem planowanej dostawy sprzętu, dokona jej awizacji, to znaczy skontaktuje się z Zamawiającym w celu ustalenia miejsca i potwierdzenia konkretnego terminu dostawy.
14. Dostawa sprzętu odbędzie się w dniu roboczym, od poniedziałku do piątku, w godzinach 8:00 - 14:00, transportem zapewnionym przez Wykonawcę, na jego koszt i ryzyko wraz z wniesieniem do miejsca wskazanego przez Zamawiającego.
15. Do czasu odbioru sprzętu przez Zamawiającego, ryzyko wszelkich niebezpieczeństw związanych z jego ewentualnym uszkodzeniem lub utratą ponosi Wykonawca.
16. Wraz ze sprzętem Wykonawca zobowiązany jest przekazać Zamawiającemu listę numerów seryjnych dostarczonych urządzeń wszelką dokumentację dostarczoną przez producenta sprzętu.
17. **Wymagania gwarancyjne.**
	1. O ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta sprzętu bądź udzielona przez autoryzowany serwis gwarancyjny producenta sprzętu. Serwis gwarancyjny musi być świadczony przez autoryzowany serwis producenta lub przez samego producenta i powinien być świadczony w miejscu instalacji sprzętu, Zamawiający nie dopuszcza udzielenia gwarancji Wykonawcy na sprzęt. Czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego (chyba że zapisy szczegółowe stanowią inaczej).
	2. Gwarantowany czas naprawy nie może być dłuższy niż 5 dni roboczych (chyba że zapisy szczegółowe stanowią inaczej). W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 15 dni roboczych od momentu zgłoszenia usterki.
	3. Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
	4. Oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej).

**UWAGA.** Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części PFU (OPZ).

1. **Miejsce instalacji i uruchomienia Systemu Informatycznego (instalacji sprzętu i oprogramowania).**

Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części PFU (OPZ), w budynku urzędu w miejscach wskazanych przez Zamawiającego.

Realizacja powyższego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

# Szczegółowe właściwości i wymagania funkcjonalno-użytkowe.

Szczegółowy opis wymagań minimalnych dla urządzeń i systemów teleinformatycznych przewidzianych w niniejszym postępowaniu przedstawiono w zestawieniu tabelarycznym.

|  |
| --- |
| 1. **Minimalne wymagania dla stacji roboczych**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | 1. W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanej stacji roboczej.
2. W ofercie należy wskazać pełną nazwę handlową zaoferowanego procesora oraz należy wskazać pełną nazwę handlową zaoferowanego systemu operacyjnego.
 |
| **Funkcjonalność obudowy** | 1. Wymagana obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej, typu SFF (Small Form Factor) umożliwiająca montaż dysku w formacie 3,5” lub 2,5” wewnątrz obudowy.
2. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco - diagnostycznym.
3. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie wpisanym na stałe w BIOS.
 |
| **Napęd optyczny** | Wymagany napęd optyczny (nagrywarka DVD +/- RW) zamontowany w dedykowanej wnęce zewnętrznej obudowy 5.25” typu slim. |
| **Zasilacz** | 1. Zasilacz o mocy max. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%,
2. Oferowany zasilacz w oferowanym komputerze musi spełniać wymóg 80 Plus (80+)
 |
| **Procesor** | Wymagany procesor klasy x86 wielordzeniowy, przystosowany na etapie produkcji do pracy w komputerach stacjonarnych, umożliwiający osiągnięcie w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik min. 8700 punktów.**Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony www.cpubenchmark.net**  |
| **Funkcjonalność płyty głównej** | Płyta główna wyposażona w co najmniej w następujące złącza (gniazda):1. 1 gniazdo PCIe x16 Gen.3,
2. 1 gniazdo PCIe x1,
3. 2 złącza SATA w tym min. 1 szt SATA 3.0,
4. 1 złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej 2 gniazda DIMM do montażu pamięci RAM
5. Moduł TPM 2.0
 |
| **Pamięć** | 1. Co najmniej 8 GB RAM z możliwością rozbudowy do min. 64 GB.
2. Co najmniej 256 GB pamięci masowej - wymagany dysk w technologii półprzewodnikowej SSD (Solid State Drive)
 |
| **Diagnostyka** | 1. Wymagana stacja robocza z systemem służącym diagnostyce wyposażonym w graficzny interfejs użytkownika, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera, a w szczególności jego składowych.System musi zapewnić pełną funkcjonalność, w szczególności zachować interfejs graficzny nawet w przypadku braku dysku twardego (lub jego uszkodzenia), nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.Procedura POST traktowana jest jako oddzielna funkcjonalność.
2. Wymagana jest stacja robocza wyposażona fabrycznie w wbudowany wizualny system diagnostyczny oparty o sygnalizację LED, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami - sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie).Zamawiający wymaga aby system był usytuowany na przednim panelu obudowy i sygnalizował co najmniej następujące stany: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora.Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji, a które nie są dedykowane dla systemu diagnostycznego.
 |
| **BIOS** | 1. Wymagany BIOS zgodny ze specyfikacją UEFI, zawierający informację o nazwie producenta komputera lub nazwie modelu oferowanego komputera. Wymagana pełna obsługa BIOS za pomocą klawiatury i myszy jak również samej myszy. BIOS musi być wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności dla następujących zmian: procesora, wielkości pamięci oraz pojemności dysku.
2. Wymagana możliwość odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio - realizowana bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych. Do odczytu wskazanych powyżej informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, itp. system diagnostyczny, czy dodatkowe oprogramowanie.
3. W ramach BIOS wymagana jest funkcjonalność polegająca na blokowaniu/ odblokowaniu BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora - użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Wymagana możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Wymagana możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB), możliwość wyłączania portów USB pojedynczo.
4. Wymagana możliwość nadania numeru inwentarzowego bezpośrednio z poziomu BIOS (bez wykorzystania dodatkowego oprogramowania), składającego się liter, cyfr oraz znaków specjalnych - wpisany numer inwentarzowy ma nie ulegać skasowaniu po aktualizacji BIOS.
5. Wymagana możliwość dokonywania backup’u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia itp.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS oraz upgrade BIOS.
 |
| **Wirtualizacja** | Wymagane sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| **Gniazda, porty, złącza** | Stacja robocza wyposażona w minimum następujące gniazda:1. 1 złącze analogowe video VGA
2. 1 wyjście cyfrowe video DisplayPort lub HDMI
3. 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie:
	1. Panel przedni: minimum 2x USB 2.0
	2. Panel tylny: minimum 4x USB 3.2 gen 1 Typu A oraz 2x USB 2.0
4. 1x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu
5. 1x port audio-out na tylnym panelu obudowy
6. 1x RJ-45

Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. |
| **Oprogramowanie dodatkowe** | Dołączone do oferowanego komputera oprogramowanie dodatkowe z nieograniczoną licencją czasową na użytkowanie umożliwiające realizację następujących funkcjonalności:1. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
2. możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem, a w szczególności informacji o:
3. poprawkach i usprawnieniach dotyczących aktualizacji
4. dacie wydania ostatniej aktualizacji
5. priorytecie aktualizacji
6. zgodność z systemami operacyjnymi
7. jakiego komponentu sprzętu dotyczy aktualizacja
8. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.
9. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne.
10. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.
11. rozpoznanie modelu oferowanego komputera, numeru seryjnego komputera, informacji kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem dokładnej daty (dd-mm-rrrr )
12. sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr ) i wersją ( rewizja wydania )
13. dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml
14. raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datę ( dd-mm-rrrr ) i godzinę z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.

Zamawiający oczekuje dostawy stacji roboczej wyposażonej w oprogramowanie zarządzające wyposażone co najmniej w następujące funkcjonalności:1. monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów
2. powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu
3. powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów

śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem. |
| **Komunikacja** | Karta sieciowa 10/100/1000 na wtyk RJ-45, wspierająca obsługęWoL |
| **Peryferia** | 1. Klawiatura w układzie polski programisty.
2. Mysz optyczna z dwoma przyciskami i rolką.
 |
| **System operacyjny** | Bezterminowa licencja oprogramowania systemu operacyjnego klasy Microsoft Windows 11 Professional lub równoważny. Za równoważny system operacyjny Zamawiający uzna system spełniający następujące minimalne parametry:1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet;
2. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
3. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW;
4. Internetowa aktualizacja zapewniona w języku polskim;
5. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych;
6. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6;
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe;
8. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi);
9. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
10. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie;
11. Praca systemu w trybie ochrony kont użytkowników;
12. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego;
13. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;
14. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie;
15. Aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;
16. Wbudowany system pomocy w języku polskim;
17. System operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
18. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
19. System posiadać powinien narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
20. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;
21. Graficzne środowisko instalacji i konfiguracji;
22. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;
23. Możliwość przywracania plików systemowych;
24. Możliwość „downgrade” do niższej wersji.

System musi być nowy (nie aktywowany wcześniej na innym urządzeniu), zainstalowany fabrycznie na dostarczonym komputerze przez producenta sprzętu. |
| **Normy, certyfikaty i standardy** | 1. Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
2. Spełnienie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
3. Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE.
 |
| **Gwarancja producenta****Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta** | W ramach wsparcia serwisowego producenta wymagany jest dedykowany portal techniczny prowadzony przez producenta lub na jego zlecenie (z bezpłatnym dostępem) służący m.in. do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi.Portal musi oferować możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego, a także możliwość pobrania aktualnych wersji sterowników oraz firmware dla stacji roboczej również w przypadku wygaśnięcia wsparcia technicznego. Portal musi mieć możliwość sprawdzenia oraz dostarczenia kompletnych danych o urządzeniu co najmniej w następującym zakresie: automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego.Dla zaoferowanej stacji roboczej Zamawiający wymaga następujących warunków gwarancji i serwisu:1. Minimalny czas trwania gwarancji udzielonej przez producenta na stację roboczą wynosi 24 miesiące.
2. W przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, uszkodzony dysk pozostaje u Zamawiającego.

Zamawiający po wyborze wykonawcy (przed podpisaniem umowy) będzie żądał złożenia oświadczenia od podmiotu realizującego serwis lub od producenta sprzętu oświadczenia potwierdzającego spełnienie w/w wymagania dla realizowanej dostawy.1. Okres zabezpieczenia serwisowego na dyski twarde, o którym mowa w pkt 2 musi odpowiadać okresowi udzielonej gwarancji na sprzęt.

Wymagana gwarancja producenta świadczona na miejscu u klienta (w przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez dział wsparcia technicznego). Wymagany czas reakcji serwisu na zgłoszenie - do końca następnego dnia roboczego. |
| **Dodatkowy okres gwarancji**(wymaganie nieobowiązkowe) | Zaoferowanie stacji roboczej z dodatkową gwarancją producenta wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium „Gwarancja (Gst)”.Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym. |

|  |
| --- |
| 1. **Minimalne wymagania dla licencji pakietu oprogramowania biurowego (edytor tekstu, arkusz kalkulacyjny, narzędzie do przygotowania prezentacji)**
 |
| Zamawiający wymaga dostawy oprogramowania w formie bezterminowej licencji oprogramowania biurowego klasy Microsoft Office lub równoważny. Za równoważny pakiet biurowy Zamawiający uzna oprogramowanie spełniające następujące minimalne wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:* 1. wymagania odnośnie interfejsu użytkownika:
* pełna polska wersja językowa interfejsu użytkownika,
* prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych;
	1. oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
* posiada kompletny i publicznie dostępny opis formatu,
* ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 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 (Dz. U. 2012, poz. 526);
	1. oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji;
	2. w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy);
	3. do aplikacji musi być dostępna pełna dokumentacja w języku polskim;

Pakiet zintegrowanych aplikacji biurowych musi zawierać: 1. Edytor tekstów,
2. Arkusz kalkulacyjny,
3. Narzędzie do przygotowywania i prowadzenia prezentacji,
4. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

Edytor tekstów musi umożliwiać: * edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
* wstawianie oraz formatowanie tabel,
* wstawianie oraz formatowanie obiektów graficznych,
* wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
* automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
* automatyczne tworzenie spisów treści,
* formatowanie nagłówków i stopek stron,
* śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie,
* nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
* określenie układu strony (pionowa/pozioma),
* wydruk dokumentów,
* wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,
* pracę na dokumentach utworzonych przy pomocy posiadanego przez Zamawiającego oprogramowania Microsoft Word 2003 lub Microsoft Word 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,
* zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,
* wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem,
* wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa;

Arkusz kalkulacyjny musi umożliwiać: * tworzenie raportów tabelarycznych,
* tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
* tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
* tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService),
* obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,
* tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
* wyszukiwanie i zamianę danych,
* wykonywanie analiz danych przy użyciu formatowania warunkowego,
* nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
* nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
* formatowanie czasu, daty i wartości finansowych z polskim formatem,
* zapis wielu arkuszy kalkulacyjnych w jednym pliku,
* zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,
* zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;

Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: * przygotowywanie prezentacji multimedialnych,
* prezentowanie przy użyciu projektora multimedialnego,
* drukowanie w formacie umożliwiającym robienie notatek,
* zapisanie jako prezentacja tylko do odczytu,
* nagrywanie narracji i dołączanie jej do prezentacji,
* opatrywanie slajdów notatkami dla prezentera,
* umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
* umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
* odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
* możliwość tworzenia animacji obiektów i całych slajdów,
* prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,
* pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint

Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: * pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
* przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
* filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
* tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
* automatyczne grupowanie poczty o tym samym tytule,
* tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
* oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
* mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
* zarządzanie kalendarzem,
* udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
* przeglądanie kalendarza innych użytkowników,
* zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
* zarządzanie listą zadań,
* zlecanie zadań innym użytkownikom,
* zarządzanie listą kontaktów, p) udostępnianie listy kontaktów innym użytkownikom,
* przeglądanie listy kontaktów innych użytkowników,
* możliwość przesyłania kontaktów innym użytkowników

Wymagana jest dostawa pakietu w najnowszej dostępnej na rynku wersji jako produkt fizyczny.W ofercie wymagane jest podanie marki (nazwy handlowej), symbolu, wersji, typu licencji, liczby licencji oferowanego oprogramowania |

|  |
| --- |
| 1. **Minimalne wymagania dla szafy teleinformatycznej Rack 42U z wyposażeniem**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | Szafa teleinformatycznaW ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanej szafy. |
| **Zastosowanie** | Do zabudowy pasywnym i aktywnym sprzętem serwerowym i sieciowym |
| **Cechy fizyczne** | Obciążalność min. 1000 kgMożliwość montażu urządzeń o sumarycznej wysokości 42UWymiary szafy: min. 800mmx1000mmx2055mm (szerokość/głębokość/wysokość)Wyposażona w 4 stopki z regulacją wysokości |
| **Konstrukcja** | Grubość materiału:Rama, góra, dół, przednie drzwi, tylne drzwi, boczne drzwi: 1,2 mmSzyny poziome: 1,5 mmSzyny pionowe: 2,0 mm |
| **Drzwi** | Drzwi przednie przeszklone (z wklejoną szybą hartowaną) z wentylowanymi bokami, wyposażone w zamek.Drzwi tylne stalowe perforowane, wentylowane, wyposażone w zamek.Zdejmowane panele boczne. |
| **Stopień ochrony** | Co najmniej IP20 |
| **Wyposażenie** | 1. Panel 4 wentylatorów z termostatem, wysokość montażowa Rack 1U.
2. Półka rackowa uniwersalna, wysokość montażowa max 1U, głębokość min. 270mm, mocowanie czteropunktowe doczołowe – min. 1 sztuka
3. Panel zaślepiający wykonany ze stali, do zaślepienia pustych przestrzeni pomiędzy urządzeniami dostarczonymi i zamontowanymi w szafie Rack w ramach realizacji niniejszego postępowania - Zamawiający wymaga aby nad urządzeniem (pod urządzeniem) znalazł się jeden panel, wysokość montażowa panela max 1U, montaż doczołowy czteropunktowy.
4. Poziomy organizer kabli, wysokość montażowa max 1U, montaż doczołowy do szyn Rack – min. 1 sztuka
5. Szafa wyposażona w zestaw śrub, podkładek, koszyków przystosowanych do montażu wewnątrz szafy pozwalający na montaż wszystkich akcesoriów takich jak: patch panele, listwy zasilające, półki do pionowych szyn w każdej szafie rack w ilości wymaganej przez zamontowane urządzenia.
 |
| **Gwarancja producenta** | Min. 24 miesiące |

|  |
| --- |
| 1. **Minimalne wymagania dla zasilacza awaryjnego UPS Online (typ 1)**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | Zasilacz awaryjny UPSW ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego zasilacza. |
| **Technologia** | TRUE ON LINE Double Conversion |
| **Moc** | 2700W (3000VA), współczynnik mocy 0,9 |
| **Wejściowy współczynnik mocy** | ≥0,99 |
| **Sprawność w trybie On-Line** | >92%  |
| **Obudowa** | 1. Wysokość obudowy max 2U - w komplecie szyny zapewniające montaż zasilacza w szafie Rack 19’’
2. Wyposażona w panel kontrolny LCD, który ma w czytelny sposób informować o trybie pracy, parametrach zasilacza, pozostałej autonomii pracy z baterii, umożliwiać konfigurację parametrów oraz pozwalać na diagnostykę zasilacza.
 |
| **Wskaźnik stanu pracy** | Panel LCD + alarm dźwiękowy |
| **Rodzaj i ilość gniazd** | Min. IEC320-C13 x8Min. IEC320-C19 x1 |
| **Start z baterii** **(tzw. zimny start)** | TAK - ma zapewnić możliwość uruchomienie zasilacza nawet w przypadku całkowitego braku napięcia zasilającego. |
| **Czas podtrzymania**  | Wymagany jest następujący czas podtrzymania zasilania realizowany za pomocą oferowanych baterii wewnętrznych dla następujących obciążeń zasilacza (wg danych z karty katalogowej producenta):1. przy 50% obciążeniu nie mniej niż 12 minut
2. przy 75% obciążeniu nie mniej niż 7 minut
 |
| **Złącze baterii zewnętrznych** | TAK - musi istnieć możliwość dołączenia jednostki rozszerzającej wyposażonej w dodatkowe łańcuchy baterii (moduł baterii) wydłużające czas podtrzymania zasilania. Zamawiający wymaga zapewnienia czasu podtrzymania przy zastosowaniu baterii wewnętrznych oraz modułu baterii zewnętrznych dla następujących obciążeń zasilacza (wg danych z karty katalogowej producenta):1. przy 50% obciążeniu nie mniej niż 42 minuty
2. przy 75% obciążeniu nie mniej niż 28 minut
 |
| **Czas ładowania** | Max. 4 godziny do 90% pojemności wg karty katalogowej producenta |
| **Cykl ładowania** | Wg DIN 41773 z automatycznym wyłączeniem ładowania wg kryterium prądu i napięcia, z kontrolą czasu. |
| **Komunikacja** | RS232, USB, TVSS, SNMP Slot, złącze REPO |
| **Pozostałe wymagania** | 1. Wraz z zasilaczem musi zostać dostarczona karta SNMP do zarządzania UPS z poziomu sieci.
2. Automatyczna diagnostyka gwarantująca pełną sprawność urządzenia, kontrolę podzespołów i parametrów pracy bez konieczności ingerencji użytkownika.
3. Odporność na przeciążenia przy występowaniu stanów nieustalonych i wysoka tolerancja na błędy obsługi.
 |
| **Normy** | Wymagane spełnienie norm w zakresie bezpieczeństwa:EN 62040-1:2008 + A1:2013, CE, EN 62040-3 :2001, EN 60950-1, EN61000-3-2 :2014  |
| **Gwarancja producenta** | Min. 24 miesiące |

|  |
| --- |
| 1. **Minimalne wymagania dla routera**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | RouterW ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego zasilacza. |
| **Obudowa** | Rack 1UW zestawie elementy montażowe pozwalające na umiejscowienie routera w szafie Rack |
| **Pamięć** | Pamięć RAM min. 4 GBPamięć wbudowana 128MB NAND |
| **Interfejsy sieciowe** | 16 gigabitowych portów Ethernet 10/100/1000 Mb/s2 sloty SFP+ (10 Gb/s) - przepustowość full duplex |
| **Porty** | 1 port 3.0 typ Aport konsolowy RJ45 |
| **Zasilanie** | 2 zasilacze (redundatne zasilanie) |
| **Wentylatory** | Aktywne chłodzenie |
| **Certyfikaty i standardy** | Oznaczenie CE |
| **Gwarancja producenta** | Min. 24 miesiące |

|  |
| --- |
| 1. **Minimalne wymagania dla konsoli KVM**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | Konsola KVMW ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanej konsoli. |
| **Obudowa** | Z możliwością instalacji w szafie Rack 19’’ - kosola nie powinna zajmować więcej niż wysokość 1U w szafie, w komplecie zestaw akcesoriów umożliwiających montaż konsoli w szafie Rack. |
| **Ilość portów** | Min. 8 portów USB/D-Sub lub PS2/D-SUB |
| **Wybór aktywnego portu** | OSD, Przycisk |
| **Ekran** | Min. 17 cali z obsługą rozdzielczości co najmniej 1280x1024 |
| **Wyposażenie** | Wbudowana pełnowymiarowa klawiatura + touchpad (płytka dotykowa)W komplecie okablowanie do każdego portu kompatybilne z oferowanym urządzeniem. |
| **Normy, certyfikaty i standardy** | Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE |
| **Gwarancja producenta** | Min. 24 miesiące |

|  |
| --- |
| 1. **Minimalne wymagania dla serwerów (typ 1)**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | Serwer.W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego serwera. |
| **Funkcjonalność obudowy** | 1. Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2. 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.
3. Wyposażona 4 porty USB z czego nie mniej niż 1 port USB 3.0, 2 porty VGA z czego jeden port video na panelu przednim.
 |
| **Procesory** | Zainstalowane dwa procesory min. 8-rdzeniowe, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 139 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.**Dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty raport z testu wydajności SPECrate®2017\_int\_base opublikowany na stronie www.spec.org dla oferowanego modelu serwera z oferowanym modelem procesora, w konfiguracji dwuprocesorowej.** |
| **Funkcjonalność płyty głównej** | Płyta główna wyposażona w minimum:1. 16 slotów (gniazd) pamięci RAM przeznaczonych do instalacji pamięci RAM.
2. 2 sloty PCIe x16 generacji 4
3. Moduł TPM 2.0
 |
| **Pamięć RAM** | Minimum 192GB z możliwością rozbudowy do 1TB pamięci RAM |
| **Funkcjonalność pamięci RAM** | Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing |
| **Interfejsy sieciowe/FC/SAS** | 1. min. 2 interfejsy sieciowe 1GbE w standardzie BaseT
2. min. 4 interfejsy sieciowe 10/25GbE SFP28
 |
| **Kable/wkładki** | 2x Kabel, SFP+ do SFP+, 10GbE, dwuosiowy kabel miedziany podłączany bezpośrednio, min. 3 metry |
| **Dyski twarde** | 1. Zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1.
2. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
 |
| **Zasilanie** | Zasilacze Redundantne, Hot-Plug min. 800W każdy. |
| **Bezpieczeństwo** | 1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
5. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie - bez potrzeby restartu serwera
6. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera - niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
 |
| **Diagnostyka** | Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
4. możliwość podmontowania zdalnych wirtualnych napędów;
5. wirtualną konsolę z dostępem do myszy, klawiatury;
6. wsparcie dla IPv6;
7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
10. integracja z Active Directory;
11. możliwość obsługi przez dwóch administratorów jednocześnie;
12. wsparcie dla dynamic DNS;
13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;
14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;
15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
 |
| **Normy, certyfikaty i standardy** | 1. Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
2. Spełnienie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
3. Spełnienie normy ISO 50001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
4. Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE.
5. Oferowany sprzęt 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 będzie wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu**.
6. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
 |
| **Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta** | 1. Serwer w ramach wymagań podstawowych musi być objęty serwisem gwarancyjnym producenta w miejscu instalacji sprzętu (dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu) przez min. 2 lata (24 miesiące), z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.
2. Wymagana jest możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.
3. W przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, uszkodzony dysk pozostaje u Zamawiającego.

Zamawiający po wyborze wykonawcy (przed podpisaniem umowy) będzie żądał złożenia oświadczenia od podmiotu realizującego serwis lub od producenta sprzętu oświadczenia potwierdzającego spełnienie w/w wymagania dla realizowanej dostawy.1. Okres zabezpieczenia serwisowego na dyski twarde, o którym mowa w pkt 1 musi odpowiadać okresowi udzielonej gwarancji na sprzęt.
2. Firma serwisująca musi posiadać wdrożone procedury zgodnie z normą ISO 9001 potwierdzone certyfikatem ISO 9001 (lub równoważnym) na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.
3. Zaoferowane serwery muszą mieć możliwość rozszerzenia gwarancji przez producenta do 7 lat.
4. Wymagana możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia.
5. Wymagana możliwość pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
6. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
 |
| **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. |
| **Dodatkowy okres gwarancji**(wymaganie nieobowiązkowe) | Zaoferowanie serwera z dodatkową gwarancją producenta wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium Gwarancja (Gs1).Zamawiający przypomina, że w przypadku zaoferowania wydłużenia gwarancji na serwer należy zaoferować okres zabezpieczenia serwisowego na dyski twarde, tożsamy z czasem gwarancji udzielonej na serwer.Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym. |

|  |
| --- |
| 1. **Minimalne wymagania dla macierzy danych**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | Macierz dyskowa.W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanej macierzy. |
| **Funkcjonalność obudowy** | Do instalacji w standardowej szafie RACK 19”, macierz musi zajmować maksymalnie 2U i pozwalać na instalacje co najmniej 24 dysków. |
| **Kontrolery** | Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów 25Gb iSCSI w standardzie SFP28 |
| **Kable/wkładki** | 4 pasywne dwuosiowe kable miedziane podłączane bezpośrednio DAC SFP28 do SFP28 min. 2m |
| **Cache** | 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii. |
| **Dyski**  | 1. Zainstalowane: 7 dysków Hot-Plug o pojemności 2.4TB SAS 12Gbps
2. Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
 |
| **Oprogramowanie, funkcjonalności** | 1. Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5.
2. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz.
3. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków.
4. Wymagana możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 8TB poprzez dyski SSD.
5. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji.
 |
| **Wsparcie dla systemów operacyjnych** | Windows Server 2022, Windows Server 2019, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi, Citrix XenServer |
| **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. |
| **Normy, certyfikaty i standardy** | 1. Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
2. Spełnienie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
3. Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE.
 |
| **Gwarancja producenta****Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta** | 1. Macierz w ramach wymagań podstawowych musi być objęta serwisem gwarancyjnym producenta lub serwisem gwarancyjnym autoryzowanego partnera serwisowego producenta w miejscu instalacji sprzętu (dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu) przez min. 24 miesiące, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.
2. Wymagana jest możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.
3. W przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, uszkodzony dysk pozostaje u Zamawiającego.

Zamawiający po wyborze wykonawcy (przed podpisaniem umowy) będzie żądał złożenia oświadczenia od podmiotu realizującego serwis lub od producenta sprzętu oświadczenia potwierdzającego spełnienie w/w wymagania dla realizowanej dostawy1. Okres zabezpieczenia serwisowego na dyski twarde, o którym mowa w pkt 1 musi odpowiadać okresowi udzielonej gwarancji na sprzęt.
2. Firma serwisująca musi posiadać wdrożone procedury zgodnie z normą ISO 9001 potwierdzone certyfikatem ISO 9001 (lub równoważnym) na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.
3. Wymagana możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia.
4. Wymagana możliwość pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.
5. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
 |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim |
| **Dodatkowy okres gwarancji**(wymaganie nieobowiązkowe) | Zaoferowanie macierzy z dodatkową gwarancją producenta wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36, lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium Gwarancja (Gm).Zamawiający przypomina, że w przypadku zaoferowania wydłużenia gwarancji na macierz należy zaoferować okres zabezpieczenia serwisowego na dyski twarde, tożsamy z czasem gwarancji udzielonej na macierz.Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym. |

|  |
| --- |
| 1. **Minimalne wymagania dla serwera backupu**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego serwera backupu. |
| **Obudowa** | Rack o wysokości max. 2U wraz z kompletem szyn teleskopowych wyposażona we wskaźniki diodowe określające następujące statusy: HDD 1-8, stan, LAN, Power, USB |
| **Pamięć** | 4GB RAM z możliwością rozbudowy do 16GB512 MB Flash32TB pamięci dyskowej (8x 4TB) wyposażonej w 128MB pamięci podręcznej dla każdego dysku |
| **Ilość obsługiwanych dysków** | 8 dysków 2.5"/3.5" SATA Hot Swap o maksymalnej pojemności 18TB każdy |
| **Interfejsy sieciowe** | 2x Port 2,5 Gigabit (2,5G/1G/100M),2x 10 GbE SFP+ |
| **Porty** | 4x USB 3.2 Gen 1, 1x PCIe Gen 2 x2 |
| **Obsługa RAID** | Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10,10+Spare,50/60.  |
| **Funkcje RAID** | Możliwość zwiększania pojemności i migracja między poziomami RAID online. Przywracanie RAID. |
| **Szyfrowanie** | Możliwość szyfrowania folderów współdzielonych oraz całych woluminów kluczem AES 256 bitów.Mechanizm szyfrowania z akceleracją sprzętową.  |
| **Obsługiwane protokoły** | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| **Usługi** | Serwer pocztowy, Stacja monitoringu, Windows ACL, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Replikacja w czasie rzeczywistym, Klient LDAP, Serwer Syslog, Migawki wolumenów, Obsługa kontenerów (LXC – Docker),Serwer VPN |
| **Zarządzanie dyskami** | SMART, sprawdzanie złych sektorów |
| **Rozszerzenie** | Możliwość rozszerzenia o maksymalnie 16 zatok |
| **Język GUI** | Polski |
| **System plików** | Dyski wewnętrzne EXT4.Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ oraz exFAT |
| **iSCSI** | Obsługa MPIO, MC/S i SPC-3 Persistent Reservation |
| **Liczba kont użytkowników** | 4096 |
| **Liczba grup** | 512 |
| **Liczba udziałów** | 512 |
| **Max ilość połączeń** | 700 |
| **Zasilanie** | Zasilacze redundatne o mocy 250W (x2) |
| **Wentylatory** | Minimum 2, o wymiarach co najmniej 70mm |
| **UPS** | Obsługa sieciowych awaryjnych zasilaczy UPS |

|  |  |
| --- | --- |
| **Gwarancja producenta****Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta** | Serwer backupowy w ramach wymagań podstawowych musi być objęty serwisem gwarancyjnym producenta lub serwisem gwarancyjnym autoryzowanego partnera serwisowego producenta w miejscu instalacji sprzętu (dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu) przez min. 24 miesiące, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. |
| **Dodatkowy okres gwarancji**(wymaganie nieobowiązkowe) | Zaoferowanie serwera backupu z dodatkową gwarancją producenta wydłużającą gwarancję podstawową o okres dodatkowych 12 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium Gwarancja (Gb).Zamawiający przypomina, że w przypadku zaoferowania wydłużenia gwarancji na serwer backupu należy zaoferować okres zabezpieczenia serwisowego na dyski twarde, tożsamy z czasem gwarancji udzielonej na macierz.Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym. |

|  |
| --- |
| 1. **Minimalne wymagania dla przełączników sieciowych zarządzalnych**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego przełącznika. |
| **Obudowa** | Do montażu w szafie Rack 19”, o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w wewnętrzny zasilacz 230V AC.  |
| **Porty** | 1. 48 portów 100M/1000M Base-T RJ45.
2. 4 porty 1G/10G SFP+.
3. Port USB umożliwiający podłączenie zewnętrznej pamięci flash.
 |
| **Wymagane mechanizmy związane z zapewnieniem bezpieczeństwa sieci** | 1. Nie mniej niż 4 poziomy dostępu administracyjnego poprzez konsolę.
2. Wymagana autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL.
3. Możliwość utworzenia minimum 2000 list ACL.
4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www.
5. Zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6.
6. Możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP.
7. Obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny) - możliwość synchronizacji czasu zgodnie z NTP.
8. Obsługa funkcjonalności DLDP lub równoważnej.
 |
| **Wymagane opcje zarządzania** | 1. Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN.
2. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC).
3. Urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych.
4. Dedykowany port konsoli musi być zgodny ze standardem RS-232.
5. Dedykowany port zarządzający out-of-band Ethernet 10/100Base-T.
 |
| **Łączenie w stos** | Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:1. Zarządzanie stosem poprzez jeden adres IP.
2. Do min. 9 jednostek w stosie.
3. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation).
4. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
 |
| **Wydajność urządzenia** | 1. Układ przełączający o wydajności min. 176 Gbps, wydajność przełączania przynajmniej 132 Mpps
2. Obsługa min. 32 000 adresów MAC
3. Wbudowana pamięć RAM min. 512 MB
4. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512 MB
5. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
6. Możliwość skonfigurowania min. 1024 interfejsów vlan interface SVI działających równocześnie
7. Obsługa ramek jumbo o wielkości min. 9216 bajtów
8. Obsługa protokołu GVRP lub równoważnego
9. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP
10. Obsługa min. 4096 tras dla routingu IPv4
11. Obsługa min. 1024 tras dla routingu IPv6
12. Obsługa protokołów routingu OSPF, OSPFv3, RIPv1, RIPv2, RIPng, PIM-SM, PIM-DM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
13. Obsługa wirtualnych tablic routingu-forwardingu (VRF)
14. Obsługa protokołów LLDP i LLDP-MED
15. Przełącznik musi posiadać funkcjonalność DHCP Server

Obsługa ruchu multicast: IGMP v1, v2 i v3, IGMP Snooping v1, v2 i v3; MLD Snooping. |
| **Obsługa ruchu sieciowego** | Wymagana implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:1. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP.
2. Wsparcie dla minimum dwóch różnych mechanizmów QoS z wykorzystaniem algorytmu karuzelowego.
3. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania.
 |
| **Pozostałe wymagania** | 1. System operacyjny (firmware) musi być dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagana pełna dokumentacja w języku polskim lub angielskim.
 |
| **Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta** | 1. Minimalny czas trwania gwarancji udzielonej przez producenta na urządzenie wynosi 36 miesięcy. Wymagane dostarczenie części zamiennych w trybie 9x5xNBD.
2. Wymagany bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
 |

|  |
| --- |
| 1. **Minimalne wymagania dla licencje na system operacyjny oraz wirtualizację, licencje dostępowe**
 |
| 1. Licencje bezterminowe (wieczyste) na oprogramowanie muszą zostać dostarczone dla każdego serwera fizycznego o którym mowa w punkcie 7. Jeśli dobór licencji zależy od liczby rdzeni procesora (procesorów) w każdym serwerze, Wykonawca ma obowiązek dostarczyć właściwą liczbę licencji dla liczby rdzeni procesora w oferowanych serwerach.
2. Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i 6 wirtualnych środowisk serwerowego systemu operacyjnego w klastrze (3 per host).
3. Zamawiający wymaga dobrania licencji w taki sposób aby przy zastosowanych procesorach umożliwić uruchomienie wskazanej liczby maszyn wirtualnych w klastrze.
4. Jeśli do legalnego korzystania z oprogramowania serwera (w zgodzie z licencją) jest wymagana licencja dostępowa (Client Access License) zapewniająca użytkownikowi prawo do korzystania z usług serwera, to należy przewidzieć dostawę sumarycznie 55 licencji dostępowych na urządzenie współpracujących z oferowanym systemem operacyjnym.
5. System musi być nowy (nie aktywowany wcześniej na innym urządzeniu).

Serwerowy system operacyjny musi posiadać następujące wymagania minimalne: 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
10. pozwalają na zmianę rozmiaru w czasie pracy systemu,
11. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
12. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
13. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
14. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
15. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
16. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
17. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
18. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
19. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
20. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
21. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
22. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
23. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
24. Mechanizmy logowania w oparciu o:
25. Login i hasło,
26. Karty z certyfikatami (smartcard),
27. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
28. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
29. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
30. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
31. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
32. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
33. Wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
34. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. 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
	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. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	4. Serwis udostępniania stron WWW.
	5. Wsparcie dla protokołu IP w wersji 6 (IPv6),
	6. Wsparcie dla algorytmów Suite B (RFC 4869),
	7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	8. budowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić 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
* Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
* Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
1. 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.
2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Zamawiający wymaga dostarczenia licencji na oprogramowanie (system serwerowy) w najnowszej wersji obecnie dostępnej na rynku.W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego oprogramowania oraz jego nazwę handlową. |

|  |
| --- |
| 1. **Wymagania minimalne dla licencje na oprogramowanie do realizacji kopii zapasowych**
 |
| 1. W ramach licencji wieczystej (bezterminowej) oprogramowanie musi zapewnić realizację kopii zapasowych z 2 (dwóch) serwerów fizycznych i 8 (ośmiu) maszyn wirtualnych.
2. Wykonawca zapewnieni wsparcie techniczne (support producenta) dla dostarczonego oprogramowania przez okres 1 roku (12 miesięcy) lecz nie dłużej niż do 30.09.2023 r.
3. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
4. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
5. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
6. 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.
 |
| **Całkowite koszty posiadania** |
| 1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
2. Oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
4. 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.
5. 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.
6. 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 takiej puli.
7. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
10. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
11. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
12. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
13. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
14. 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.
15. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
16. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
17. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych
 |
| **Wymagania RPO** |
| 1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
2. Oprogramowanie musi wykorzystywać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
4. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru.
5. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
6. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
7. Oprogramowanie musi posiadać wsparcie dla NDMP
8. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
9. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
10. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
11. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
12. Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
13. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
14. 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.
15. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
16. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
17. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
18. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
 |
| **Wymagania RTO** |
| 1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
2. Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.
5. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
7. Oprogramowanie musi umożliwić odtworzenie plików 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.
8. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
9. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
10. Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
11. BSD: UFS, UFS2
12. Solaris: ZFS, UFS
13. Mac: HFS, HFS+
14. Windows: NTFS, FAT, FAT32, ReFS
15. Novell OES: NSS
16. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
17. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
18. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
19. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
20. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
21. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska.
22. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
23. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska.
24. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych.
25. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
26. 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.
27. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.
28. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
29. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
30. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
 |
| **Ograniczenie ryzyka** |
| 1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
2. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
4. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere.
5. 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.
6. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
 |
| **Monitoring** |
| 1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 - zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
4. System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez Vmware.
5. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
6. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
7. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.
8. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
9. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
10. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
11. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
12. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
13. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
14. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
15. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
16. 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.
17. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
18. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x.
 |
| **Raportowanie** |
| 1. System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019
2. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
3. System musi być certyfikowany przez VMware i posiadać status „VMware Ready”.
4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.
5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.
6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
11. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie
 |
| **Agent** |
| 1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux:
	* Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
4. Rozwiązanie musi wspierać systemy operacyjne macOS
5. Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików:
	* NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2
6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
9. Rozwiązanie musi wspierać backup podłączonych dysków USB
10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na:
	* 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.
	* Zcentralizowanym repozytorium danych
	* Bezpośrednio na zasobach Chmury
12. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
13. Rozwiązanie musi wspierać kontrolę pasma sieciowego
14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
17. Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
18. Rozwiązanie musi wspierać technologię BitLocker
19. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
20. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla:
	* Microsoft Exchange 2010 i nowszych
	* Microsoft Active Directory 2003 i nowszych
	* Microsoft Sharepoint 2010 i nowszych
	* Microsoft SQL 2005 i nowszych
	* Oracle 11g i nowszych
21. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
22. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
23. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2
24. Rozwiązanie musi wspierać szyfrowanie
25. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
26. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
27. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
28. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.
 |

|  |
| --- |
| 1. **Minimalne wymagania dla serwera (typ 2)**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | Serwer dla jednostki podległej.W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego serwera. |
| **Obudowa** | Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| **Płyta główna** | Płyta główna wyposażona w minimum 4 sloty przeznaczone do instalacji pamięci, z możliwością obsługi 128GB pamięci RAM. |
| **Procesor** | Wymagany procesor klasy x86 wielordzeniowy, przystosowany na etapie produkcji do pracy w serwerach, umożliwiający osiągnięcie w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik min. 18000 punktów**Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony www.cpubenchmark.net** |
| **Pamięć operacyjna** | Co najmniej 32GB RAM |
| **Gniazda PCI** | Minimum dwa sloty PCIe generacji 4 |
| **Interfejsy sieciowe** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT |
| **Dyski twarde** | 1. Zainstalowane 2 dyski SAS o pojemności min. 600GB, 12Gb, Hot-Plug
2. Wymagana możliwość instalacji dysków SAS, SATA, SSD, NL SAS
3. Wymagana możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
4. Wymagana możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
 |
| **Kontroler dysków** | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10 |
| **Wbudowane porty** | 4x USB z czego nie mniej niż 1x USB 3.0, 1x VGA, 1x RS232 |
| **Zasilacze** | Zasilacz o mocy max 450W. |
| **Napęd optyczny** | Wbudowany napęd DVD +/- RW |
| **Bezpieczeństwo** | 1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
2. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
3. Wymagany moduł TPM 2.0 pełniący funkcję dodatkowej warstwy sprzętowej do obsługi różnych działań kryptograficznych, w tym do ochrony kluczy szyfrowania, danych uwierzytelniania i innych wrażliwych danych.
 |
| **Diagnostyka** | Wymagana możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
4. wsparcie dla IPv6;
5. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
6. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
7. wsparcie dla dynamic DNS;
8. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;
9. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;
10. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
 |
| **Normy, certyfikaty i standardy** | 1. Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
2. Spełnienie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
3. Spełnienie normy ISO 50001 lub równoważnej dla producenta sprzętu - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.
4. Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE.
5. Oferowany model serwera musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
 |
| **Gwarancja producenta****Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta** | 1. Serwer w ramach wymagań podstawowych musi być objęty serwisem gwarancyjnym producenta w miejscu instalacji sprzętu (dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu) przez min. 2 lata (24 miesiące), z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.
2. Wymagana jest możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.
3. W przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, uszkodzony dysk pozostaje u Zamawiającego.

Zamawiający po wyborze wykonawcy (przed podpisaniem umowy) będzie żądał złożenia oświadczenia od podmiotu realizującego serwis lub od producenta sprzętu oświadczenia potwierdzającego spełnienie w/w wymagania dla realizowanej dostawy.1. Okres zabezpieczenia serwisowego na dyski twarde, o którym mowa w pkt 1 musi odpowiadać okresowi udzielonej gwarancji na sprzęt.
2. Firma serwisująca musi posiadać wdrożone procedury zgodnie z normą ISO 9001 potwierdzone certyfikatem ISO 9001 (lub równoważnym) na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.
3. Zaoferowane serwery muszą mieć możliwość rozszerzenia gwarancji przez producenta do 7 lat.
4. Wymagana możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia.
5. Wymagana możliwość pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
6. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
 |
| **Dodatkowy okres gwarancji**(wymaganie nieobowiązkowe) | Zaoferowanie serwera z dodatkową gwarancją producenta wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium Gwarancja (Gs2).Zamawiający przypomina, że w przypadku zaoferowania wydłużenia gwarancji na serwer należy zaoferować okres zabezpieczenia serwisowego na dyski twarde, tożsamy z czasem gwarancji udzielonej na serwer.Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym. |
| **System operacyjny** | Oprogramowanie musi zostać dostarczone dla serwera fizycznego wyposażonego w 1 procesor wielordzeniowy. Jeśli dobór licencji zależy od liczby rdzeni procesora, Zamawiający ma obowiązek dostarczyć właściwą liczbę licencji dla liczby rdzeni procesora w oferowanym serwerze. Wraz z licencją na system operacyjny wymagane jest dostarczenie nośnika CD/DVD zawierającego pakiet instalacyjny oferowanego systemu.Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i min. jednego wirtualnego środowiska serwerowego systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 64GB pamięci RAM w środowisku fizycznym.
2. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
3. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
4. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
5. pozwalają na zmianę rozmiaru w czasie pracy systemu,
6. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
7. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
8. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
10. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
11. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
15. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
16. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
17. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
18. Mechanizmy logowania w oparciu o:
19. Login i hasło,
20. Karty z certyfikatami (smartcard),
21. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
22. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
23. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
24. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
25. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
26. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
27. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
28. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
29. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
30. 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
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. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
4. Serwis udostępniania stron WWW.
5. Wsparcie dla protokołu IP w wersji 6 (IPv6),
6. Wsparcie dla algorytmów Suite B (RFC 4869),
7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
8. 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.
9. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
 |

|  |
| --- |
| 1. **Minimalne wymagania dla zasilacza awaryjnego UPS Online (typ 2)**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | Zasilacz awaryjny UPSW ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego zasilacza. |
| **Technologia** | TRUE ON LINE Double Conversion |
| **Moc** | 2700W (3000VA), współczynnik mocy 0,9 |
| **Wejściowy współczynnik mocy** | ≥0,99 |
| **Sprawność w trybie On-Line** | >92%  |
| **Obudowa** | 1. Wysokość obudowy max 2U - w komplecie szyny zapewniające montaż zasilacza w szafie Rack 19’’
2. Wyposażona w panel kontrolny LCD, który ma w czytelny sposób informować o trybie pracy, parametrach zasilacza, pozostałej autonomii pracy z baterii, umożliwiać konfigurację parametrów oraz pozwalać na diagnostykę zasilacza.
 |
| **Wskaźnik stanu pracy** | Panel LCD + alarm dźwiękowy |
| **Rodzaj i ilość gniazd** | Min. IEC320-C13 x8Min. IEC320-C19 x1 |
| **Start z baterii** **(tzw. zimny start)** | TAK - ma zapewnić możliwość uruchomienie zasilacza nawet w przypadku całkowitego braku napięcia zasilającego. |
| **Czas podtrzymania**  | Wymagany jest następujący czas podtrzymania zasilania realizowany za pomocą oferowanych baterii wewnętrznych dla następujących obciążeń zasilacza (wg danych z karty katalogowej producenta):1. przy 50% obciążeniu nie mniej niż 12 minut
2. przy 75% obciążeniu nie mniej niż 7 minut
 |
| **Czas ładowania** | Max. 4 godziny do 90% pojemności wg karty katalogowej producenta |
| **Cykl ładowania** | Wg DIN 41773 z automatycznym wyłączeniem ładowania wg kryterium prądu i napięcia, z kontrolą czasu. |
| **Komunikacja** | RS232, USB, TVSS, SNMP Slot, złącze REPO |
| **Pozostałe wymagania** | 1. Automatyczna diagnostyka gwarantująca pełną sprawność urządzenia, kontrolę podzespołów i parametrów pracy bez konieczności ingerencji użytkownika.
2. Odporność na przeciążenia przy występowaniu stanów nieustalonych i wysoka tolerancja na błędy obsługi.
 |
| **Normy** | Wymagane spełnienie norm w zakresie bezpieczeństwa:EN 62040-1:2008 + A1:2013, CE, EN 62040-3 :2001, EN 60950-1, EN61000-3-2 :2014  |
| **Gwarancja producenta** | Min. 24 miesiące |

|  |
| --- |
| 1. **Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Usługi** | Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji projektu, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa. Po zapoznaniu się z architekturą sieciową urzędu Wykonawca przedstawi plan reorganizacji sieci oraz wirtualizacji z uwzględnieniem istniejącego i dostarczanego sprzętu. Schemat ten musi być uzgodniony z Zamawiającym i uwzględniać jego wytyczne.Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych.Zamawiający wymaga sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia.Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Dokumentacją Powykonawczą. |
| **Montaż i fizyczne uruchomienie systemu** | Zamawiający wymaga zainstalowania wskazanego, dostarczonego rozwiązania w pomieszczeniu serwerowni, lub w innych wskazanych miejscach co najmniej w następującym zakresie:1. Wniesienie, ustawienie i fizyczny montaż szafy Rack w pomieszczeniu wskazanym przez Zamawiającego.
2. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń:
3. dla Urzędu Gminy: Zasilacz awaryjny UPS, onsola KVM, serwery (typ1), macierz, serwer backupowy, urządzenia sieciowe (przełączniki, router, urządzenie firewall).
4. Dla jednostki podległej: serwer (typ2), UPS (typ2)
5. Urządzenia, które nie są montowane w szafach teleinformatycznych np.: komputery, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
6. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
7. Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
8. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
9. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
10. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami zamontowanymi w szafie Rack, w celu zapewnienia komunikacji - Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane (min. kat. 6 UTP) lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
11. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające do szafy Rack).
12. Demontaż „starych” urządzeń IT z szafy teleinformatycznej, które nie będą już wykorzystywane.
13. Po wykonaniu instalacji przeprowadzenie testów sprawdzających poprawność instalacji i działania urządzeń.
 |
| **Konfiguracja routera** | Wykonawca przeprowadzi konfigurację routera w sposób uzgodniony z Zamawiającym poprzez ustawienie niezbędnego poziomu bezpieczeństwa, zablokowanie dostępu przez osoby nieuprawnione, dopasowanie protokołów i ustawień do architektury sieci w Urzędzie Gminy. |
| **Konfiguracja przełączników sieci LAN:** | Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi wskazanymi urządzeniami sieciowymi. Centralnym punktem będzie serwerownia zlokalizowana w Urzędzie Gminy (Miejsce instalacji przełączników sieci LAN).Przełączniki będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego). Wykonawca przeprowadzi konfigurację dostarczanych przełączników w zakresie:1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
2. Konfiguracja sieci wirtualnych VLAN, taka liczba sieci wirtualnych aby odseparować różne typy ruchu, w porozumieniu z Zamawiającym.
3. Konfiguracja połączeń pomiędzy istniejącymi przełącznikami z wykorzystaniem połączeń światłowodowych oraz miedzianych (utworzenie agregacji na wspieranych urządzeniach).
4. Konfiguracja routingu pomiędzy sieciami VLAN na firewall’u.
5. Testowanie obsługi ruchu sieciowego.
6. Testowanie skuteczności zabezpieczeń.
 |
| **Konfiguracja elementów bezpieczeństwa sieciowego** | Urządzenie firewall:1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.
3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email)
4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu gminy
5. Konfiguracja dostarczonego systemu Firewall:
	1. Konfiguracja podstawowych parametrów
	2. Konfiguracja translacji adresów NAT
	3. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, serwery komunikacyjne telefonii IP, itp.
	4. Konfiguracja inspekcji określonych protokołów sieciowych;
	5. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;
	6. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
	7. Testowanie działania bramy
6. Konfiguracja modułów należących do systemu wykrywania włamań IPS:
	1. Konfiguracja podstawowych parametrów
	2. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;
	3. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;
	4. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
	5. Testowanie działania ochrony IPS
7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.
	1. Przypisanie adresu IP do zarządzania.
	2. Konfiguracja inspekcji protokołów HTTP, SMTP, FTP, POP3
	3. Definicja reguł filtrowania/blokowania
8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej z uwierzytelnieniem w oparciu o usługę katalogową.
9. Uruchomienie i skonfigurowanie instancji systemów bezpieczeństwa dla skonfigurowanych sieci wirtualnych VLAN, taka liczba sieci wirtualnych aby odseparować różne typy ruchu, w porozumieniu z zamawiającym.
10. W instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności:
	1. kontrola dostępu - zapora ogniowa klasy Statless Inspection
	2. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar
	3. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
	4. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
	5. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
	6. kontrola pasma oraz ruchu [QoS, Traffic shaping]
	7. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
	8. Ochrona przed wyciekiem poufnej informacji (DLP)
	9. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL)
	10. Inspekcja ruchu SSL
	11. Ochrony przez atakami na stacje klienckie
	12. Kontrola pasma
11. Konfiguracja logowania i raportowania.
12. Konfiguracja logowania i raportowania do alternatywnego serwera SYSLOG uruchomionego na serwerze NAS (instalacja i konfiguracja serwera SYSLOG spoczywa na Wykonawcy). Jeśli dla zapewnienia tej funkcjonalności wymagane są jakiekolwiek licencje - ich dostarczenie spoczywa na Wykonawcy.
 |
| **Reorganizacja i porządkowanie** | Po zapoznaniu się z architekturą sieciową Urzędu Gminy i przedstawieniu schematu reorganizacji sieci z uwzględnieniem istniejącego i dostarczanego sprzętu zaakceptowanego przez Zamawiającego, Wykonawca przeprowadzi porządkowanie połączeń wewnętrznych. |
| **Instalacja i konfiguracja serwerów, instalacja systemu operacyjnego serwerów** | Fizyczna instalacja dwóch serwerów (typ 1) w szafie Rack. Konfiguracja odpowiedniego poziomu RAID wskazana przez Zamawiającego. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Instalacja niezbędnych aktualizacji oraz poprawek związanych z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.Fizyczna instalacja serwera (typ 2) w miejscu wskazanym przez Zamawiającego.Konfiguracja odpowiedniego poziomu RAID wskazana przez Zamawiającego. Instalacja niezbędnych aktualizacji oraz poprawek związanych z bezpieczeństwem udostępnione przez producenta systemu operacyjnego. |
| **Uruchomienie środowiska wirtualizacyjnego** | Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w następującym zakresie:1. Aktywacja licencji oprogramowania wirtualizacyjnego
2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego - aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
3. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach (typ 1).
4. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.
5. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
6. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.
7. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.
8. Przygotowania koncepcji i wykonania wirtualizacji do 6 wirtualnych maszyn z przeniesieniem systemów używanych w Urzędzie Gminy.
9. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.
10. Konfiguracja klastra wysokiej dostępności:
	1. Konfiguracja mechanizmów HA - w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika.
	2. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.
	3. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera.
11. Weryfikacja działania klastra wysokiej dostępności.
12. Migracja istniejącej infrastruktury do środowiska wirtualnego.
 |
| **Uruchomienie usługi katalogowej oraz niezbędnych komponentów, migracja danych do/z obecnej usługi katalogowej** | Uruchomienie usługi katalogowej na dwóch wirtualnych systemach, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na serwerach wraz z komponentami odpowiedzialnymi za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowany system operacyjny, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem.Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:1. Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości
2. Śledzenie zmian dotyczących tworzenia, usuwania obiektów

Zamawiający wymaga skonfigurowania jednej stacji zarządzającej. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów). |
| **Konfiguracja polityki haseł oraz polityki blokowania kont** | Konfiguracja globalnej polityki haseł dla domeny:1. Hasło musi zawierać minimum 8 znaków
2. Maksymalny czas ważności hasła: do ustalenia z Zamawiającym
3. Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym
4. Hasło musi spełniać zasady złożoności

Konfiguracja polityki haseł dla kadry zarządzającej:1. Hasło musi zawierać minimum 10 znaków
2. Maksymalny czas ważności hasła: 30 dni
3. Minimalny czas, po którym możliwa jest zmiana hasła: 30 dni
4. Hasło musi spełniać zasady złożoności
5. Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach.

Szczegółowe dane zostaną przekazane na etapie konfiguracji. |
| **Uruchomienie i konfiguracja systemu zarządzania kopiami zapasowymi** | Instalacja oraz uruchomienie dostarczonego środowiska wykonywania kopii zapasowych (serwer backupowy NAS) oraz aktywacja wymaganych licencji.Wymagana będzie konfiguracja zadań wykonywania kopii zapasowych wirtualnych maszyn według poniższych wymagań:1. Kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;
2. Kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;
3. Kopie maszyn wirtualnych muszą być replikowane na wskazany przez Zamawiającego zasób dyskowy;
4. Kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;
5. Kopie zapasowe muszą (jeżeli jest taka funkcjonalność) być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;
6. Musi istnieć możliwość odtworzenia: całej wirtualnej maszyny, dysku wirtualnej maszyny, pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa);

Oprogramowanie musi umożliwiać: 1. Replikację maszyn wirtualnych w oparciu o obrazy.
2. Syntetyczną pełną kopię zapasową - tworzenie kopii zapasowych forever-incremental.
3. Tworzenie harmonogramów kopii zapasowych bezpośrednio z UI.
4. Weryfikacja kopii zapasowej pod kątem infekcji i złośliwego oprogramowania przed przywróceniem do środowiska produkcyjnego.
5. Konfiguracja powiadomień o wykonaniu kopii zapasowej (e-mail).

Rozwiązanie zostanie poddane testowaniu poprzez:1. Uruchomienie testowych zadań backupu.
2. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email.
3. Uruchomienie testowych zadań odtworzenia danych.
 |
| **Dołączenie stacji roboczych do domeny** | Zamawiający wymaga dołączenia wszystkich dostarczonych oraz istniejących, kwalifikujących się stacji roboczych do domeny. W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mających na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (między innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na konto domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji). |
| **Migracja systemów** | Zamawiający wymaga przeniesienia systemów wykorzystywanych w UG na nowe, zainstalowane i skonfigurowane wirtualne systemy bądź zwirtualizuje fizyczne systemy UG.Po wykonaniu migracji zostaną przeprowadzone testy sprawdzające poprawność wykonania czynności. |
| **Wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.** | Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą. |
| **Opracowanie dokumentacji powykonawczej** | Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej)  |
| **Poziom usług**(wymaganie dodatkowe, fakultatywne) | W celu zapewnienia wysokiego poziomu wykonywanych zadań, podmiot realizujący usługi informatyczne przedstawione w niniejszym rozdziale w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania powinien posiadać wdrożony system zarządzania jakością potwierdzony aktualnym certyfikatem ISO 9001 w zakresie świadczenia usług w obszarze bezpieczeństwa teleinformatycznego i/lub cyberbezpieczeństwa - wymaganie ma charakter fakultatywny.Za spełnienie wymagania wykonawca otrzyma dodatkową liczbę punktów w kryteriach poza cenowych zgodnie z warunkami (kryteriami) opisanymi w SWZ.Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę certyfikat ISO przyznany przez niezależną jednostkę certyfikującą |

|  |
| --- |
| 1. **Wymagania minimalne dla szkoleń stacjonarnych dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania**
 |
| * + - 1. Wykonawca w okresie wdrożenia przeprowadzi w siedzibie Zamawiającego podstawowe szkolenie dla Administratorów systemu (dla 2 osób), w wymiarze min. 18 godzin szkolenia (3 dni robocze). Szkoleniem zostaną objęte osoby wskazane przez Zamawiającego z zakresie dostarczonego rozwiązania teleinformatycznego, co najmniej w zakresie:
1. Obsługi dostarczonych serwerów, macierzy dyskowej oraz utrzymania klastra HA.
2. Zarządzania systemami serwerowymi oraz wirtualizacją.
3. Obsługi dostarczonego serwera backupu, archiwizacji danych oraz wykonywania kopii zapasowych.
4. Zarządzania routerem oraz przełącznikami sieciowymi.

Celem szkolenia administratorów będzie zapoznanie się z systemem informatycznym, poznanie poszczególnych funkcji i modułów oraz nauka jego obsługi w praktyce. Na etapie wdrożenia, strony ustalą szczegółowy porządek i podział szkoleń z uwzględnieniem wymagań zawartych w niniejszym rozdziale, które przyjęte zostaną w planie szkoleń.Wykonawca zobowiązany jest do przeprowadzenia szkoleń w formie instruktażu stanowiskowego dla personelu w siedzibie Zamawiającego.* + - 1. Wykonawca w okresie wdrożenia zorganizuje szkolenie dla Administratorów systemu (dwie osoby) z praktycznej obsługi i podstawowej konfiguracji systemu bezpieczeństwa firewall (dostarczonego urządzenia firewall) w formie warsztatów, łącznie w wymiarze co najmniej 2 dni szkoleniowych. Zamawiający dopuszcza odbycie szkoleń w miejscu wskazanym przez Wykonawcę na terenie województwa podkarpackiego, w którym Zamawiający ma swoją siedzibę.

Zamawiający dopuszcza odbycie szkoleń poza terenem województwa podkarpackiego, w miejscu wskazanym przez Wykonawcę w promieniu do 250 km licząc od siedziby Zamawiającego. W przypadku zaoferowania odbycia warsztatów poza terenem województwa podkarpackiego, w którym Zamawiający ma swoją siedzibę obowiązkiem Wykonawcy jest zapewnienie noclegu oraz wyżywienia dla personelu Zamawiającego przez Wykonawcę (realizatora szkoleń) w miejscu realizacji szkoleń.Plan szkolenia z obsługi i konfiguracji systemu bezpieczeństwa firewall powinien obejmować:1. Wstępne informacje o platformie
2. Przywracanie ustawień domyślnych
3. Wstępną konfigurację
4. Aktualizację oprogramowania
	1. Aktualizacja oprogramowania poprzez interfejs graficzny GUI
	2. Aktualizacja oprogramowania poprzez CLI
5. Metody zarządzania platformą
	1. Omówienie interfejsu GUI, Features
	2. Omówienie interfejsu CLI
6. Rejestrację urządzeń, konto supportowe
7. Debugowanie komunikacji z siecią
8. Akcelerację sprzętowa w platformach
9. Logowanie
10. Analizę aktywności w sieci
11. Analiza rozwiązywania problemów (sesje, sniffer, flow) - backup konfiguracji.
	1. Tcpdump ruchu
	2. Analiza flow ruchu
	3. Wyświetlanie informacji o sesjach
	4. Wireshark tworzenie pliku
	5. Backup Konfiguracji
12. Konfiguracja SD-WAN
	1. Techniki balansowania
	2. SD-WAN Status Check
	3. SD-WAN Rules
13. Kontrola AV - Techniki skanowania
	1. Konfiguracja skanowania AV
	2. Konfiguracja Sandbox-a
	3. Konfiguracja CDR
	4. Konfiguracja Malware Hash
14. Analiza ruchu szyfrowanego SSL
	1. Konfiguracja profilu sprawdzania certyfikatów
	2. Konfiguracja profilu analizy ruchu szyfrowanego
15. Kontrola aplikacji
16. Konfiguracja Webfiltering’u
	1. White/Black listy lokalne repozytorium
	2. White/Black listy zewnętrzne repozytora
17. DNS filter

Szkolenie powinno być dedykowane dla administratorów (specjalistów z zakresu sieci i bezpieczeństwa) zajmujących się zarządzaniem, konfiguracją, administracją i monitorowaniem urządzeń klasy firewall w Urzędzie. Zamawiający wymaga aby podczas szkolenia administratorzy uzyskali wiedzę praktyczną z podstawowych funkcjonalności zaoferowanego przez Wykonawcę urządzenia klasy Firewall. Zdobyte umiejętności mają zapewnić administratorowi niezbędna wiedzę i umiejętności pozwalające na samodzielną konfigurację co najmniej na poziomie podstawowym szeregu elementów kompletnego systemu bezpieczeństwa sieci.* + - 1. W okresie wdrożenia Wykonawca zorganizuje certyfikowane szkolenie dla Administratora systemu (jedna osoba) z praktycznej obsługi oprogramowania specjalistycznego o którym mowa w punkcie 18, łącznie w wymiarze co najmniej 2 dni szkoleniowych. Zamawiający dopuszcza odbycie szkoleń w miejscu wskazanym przez Wykonawcę w promieniu do 250 km licząc od siedziby Zamawiającego.

Plan szkolenia z obsługi i konfiguracji oprogramowania specjalistycznego powinien obejmować:* + - 1. Ogólne omówienie programu.
			2. Wymagania i instalacja systemu.
			3. Wstępna konfiguracja systemu i instalacja.
			4. Konfiguracja i praca we wszystkich modułach dostarczonych w ramach niniejszego projektu.
			5. Rozwiązywanie najczęstszych problemów.
			6. Egzamin certyfikujący.

Obowiązkiem Wykonawcy będzie zapewnienie:1. Szkoleń (warsztatów) w formie stacjonarnej prowadzonych przez wieloletniego praktyka i szkoleniowca,
2. Pakietu materiałów szkoleniowych,
3. W trakcie szkoleń: Lunch + przerwy kawowe,
4. Jednego noclegu ze śniadaniem,
5. Odbycia egzaminu zakończonego certyfikatem.

Podczas szkolenia (warsztatów) administrator ma:1. Zdobyć kompleksową wiedzę niezbędną do skutecznego zarządzania siecią w urzędzie;
2. Poznać najważniejsze funkcjonalności zakupionego specjalistycznego oprogramowania;
3. Zdobyć wiedzę jak poprawnie skonfigurować i korzystać z poszczególnych modułów programu;
4. Zdobyć wiedzę jak monitorować krytyczne urządzenia, usługi czy procesy tak aby zdobyć odpowiednią wiedzę o architekturze sieci, działaniu poszczególnych jej komponentów oraz jej wydajności i pojemności.
5. Zdobyć umiejętności do zapanowania nad niejednolitą konfiguracją programową i sprzętową swoich stacji, wykonania audytu oprogramowania, plików multimedialnych, zwiększenia swoich umiejętności w obszarze zarządzania środkami trwałymi.
6. Zdobyć umiejętności w obszarze monitorowania aktywności użytkowników, tak aby można było szybko i jednoznacznie analizować ich pracę i jednocześnie dbać o bezpieczeństwo organizacji.
7. Zdobyć umiejętności pozwalające na rozliczalność komunikacji „użytkownik-IT”, na zbudowanie bazy wiedzy dla pracowników, na zautomatyzowanie procesów związanych z obsługą zgłoszeń serwisowych.
8. Zdobyć umiejętności w zakresie zarządzania nośnikami zewnętrznymi, rozliczania pracy z nimi oraz rozliczania pracy na plikach wspólnych.
9. Zdobyć umiejętności jak skonfigurować program pod indywidualne potrzeby, zdefiniować rozpraszacze oraz w łatwy sposób udostępnić wskaźniki aktywności pracownikom oraz przełożonym, aby zwiększyć ich świadomość dotyczącą wykorzystania czasu.
10. Zdobyć umiejętność skonfigurowania widżetów prezentujących kluczowe parametry, historię pracy sieci oraz informacje o działaniach użytkowników.
11. Szkolenie (warsztaty) muszą zakończyć się uzyskaniem certyfikatu „Certified Administrator” wydanym przez jednostkę organizującą szkolenie.
 |

|  |
| --- |
| 1. **Wymagania minimalne dla szkoleń dla pracowników urzędu z cyberbezpieczeństwa**
 |
| W ramach realizacji niniejszego projektu Zamawiający wymaga zorganizowania przez Wykonawcę szkoleń mających na celu podniesienie świadomości pracowników urzędu z zakresu cyberbezpieczeństwa oraz budowania umiejętności radzenia sobie z cyberzagrożeniami. W związku z tym, że podstawowym warunkiem skutecznej ochrony informacji jest świadomość osób je przetwarzających, podczas realizacji cyklu szkoleń pracownicy powinni zdobyć podstawową wiedzę i nowe umiejętności lub usprawnić już posiadane wzorce zachowań. Celem, który Zamawiający chce osiągnąć jest podniesienie świadomości pracowników w zakresie ochrony danych wrażliwych w organizacji oraz uświadomienie rzeczywistych zagrożeń płynących ze strony przestępców działających w sieci, a także ryzyka dla informacji i reputacji organizacji oraz przeciwdziałanie zagrożeniom płynącym z sieci.Wymagana jest realizacja szkoleń stacjonarnych realizowanych w formie wykładu w siedzibie Zamawiającego.* + - * 1. Wstęp teoretyczny, wprowadzający podstawowe pojęcia, uświadamiający rolę pracowników jednostki w kształtowaniu bezpieczeństwa organizacji.
				2. Wykład omawiający działanie, metody, trendy oszustw internetowych oraz podstawowe metody obrony.

Opis szkolenia:1. Jednostką czasową szkolenia będzie godzina szkoleniowa = 45 min.
2. Szkolenia stacjonarne dla każdej z grup nie powinny trwać dłużej niż 3 godziny szkoleniowe (3x 45 minut).
3. Przewidywana jest jedna przerwa 15 min, realizowana po 2 godzinach szkoleniowych (przerwa nie wlicza się w godziny szkoleniowe).
4. Szkolenia będą odbywać się w dni robocze w godzinach 7.30 - 15.30.
5. Szkolenia będą prowadzone w języku polskim.
6. Szkolenia będą realizowane w terminie ustalonym wspólnie z Zamawiającym.
7. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego harmonogramu szkoleń:
8. harmonogram szkoleń zostanie opracowywany wspólnie z Zamawiającym,
9. szkolenia nie muszą być prowadzone w jednym cyklu,
10. harmonogram szkoleń powinien być zaakceptowany przez Zamawiającego nie później niż 4 dni przed rozpoczęciem szkolenia.
11. Szkolenia będą prowadzone na podstawie zaakceptowanego prze Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
12. W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach oraz ustali skład grup - w przypadku nieobecności uczestnika na zajęciach prowadzonych w ramach jego grupy szkoleniowej, może dołączyć do innej grupy.
13. W ramach organizacji szkoleń Wykonawca zapewni:
14. Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia.
15. Wydanie uczestnikom szkolenia zaświadczeń o ukończeniu szkolenia.
16. Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
17. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
* Lista obecności uczestników szkolenia (prowadzona oddzielnie dla każdej

grupy);* Lista potwierdzająca odbiór zaświadczeń o ukończeniu szkolenia;
* Potwierdzenie przez uczestników odbioru materiałów szkoleniowych;
* Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe;
* Informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

**Dodatkowe informacje:*** + - 1. Szkolenia odbędą się z podziałem na grupy.
			2. Szkolenia odbędą się w lokalu udostępnionym przez Zamawiającego z dostępem do Internetu, ogrzewania oraz energii elektrycznej.
			3. Sprzęt elektroniczny (laptop, projektor) niezbędny do prowadzenia szkolenia zapewnia Wykonawca.

**Zakres szkolenia:**1. Główne założenia i wymagania prawne RODO, KRI, KSC.
2. Incydent bezpieczeństwa komputerowego i RODO - zasady postepowania w przypadku jego wystąpienia.
3. Naruszenie ochrony danych osobowych i zasady postepowania w przypadku jego wystąpienia.
4. Podstawowe zasady bezpieczeństwa (bezpieczeństwo fizyczne):
	1. Zasada czystego biurka;
	2. Zasada czystego ekranu;
	3. Zasada czystego wydruku;
	4. Zasada czystego kosza;
5. Polityka bezpiecznych haseł (menadżer haseł, generowanie i dobór haseł, postępowanie z hasłami).
6. Najczęściej wykorzystywane metody ataków (socjotechnika, phishing, spoofing, sim swap, ataki przez strony www, telefon, spam).
7. Podstawowe metody obrony i weryfikacji prób ataków.
8. Omówienie ataków na przykładach.
9. Rozmowa otwarta - podsumowanie szkolenia.
 |

|  |
| --- |
| 1. **Wymagania minimalne dla specjalistycznego oprogramowania**
 |
| Oprogramowanie specjalistyczne musi posiadać budowę modułową i musi składać się z serwera zarządzającego, zdalnych konsoli oraz agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami musi być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.Oprogramowanie powinno wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source bez limitu ilości danych. W przypadku dostarczenia oprogramowania pracującego na komercyjnej bazie danych, rolą Wykonawcy jest dostarczenie właściwej liczbę licencji dla systemu bazodanowego umożliwiającą działanie zaoferowanego oprogramowania w opisywanym zakresie.Zamawiający wymaga dostarczenia oprogramowania z interfejsem w języku polskim wraz z podręcznikiem użytkownika (dopuszczona jest podręcznik w w postaci strony internetowej).Zamawiający wymaga dostarczenia licencji wieczystej na oprogramowanie umożliwiające jego zastosowane dla 49 stacji roboczych wg następującego podziału:- 1 dostęp administracyjny- 37 stacji roboczych w Urzędzie Gminy- 7 stacji roboczych w GOPS- 5 stacji roboczych w CUWoraz zapewnienia min. 12 miesięcy (lecz nie dłużej niż do 30.09.2023) wsparcia technicznego ze strony producenta obejmującego pomoc techniczną oraz aktualizacje oprogramowania.W ramach oprogramowania musi zostać zapewniona funkcjonalność polegająca na usuwaniu danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej - dane, które dotyczą działań pracownika na komputerze, takich jak: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Dane te powinny być grupowane w dedykowanym oknie.Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów - w programie musi istnieć możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji programu, grup urządzeń, jak i użytkowników.Główny Administrator musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do opcji programu oraz logów działań innych administratorów. Działania administratorów muszą być logowane oznacza to, że program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów powinny być automatycznie eksportowane do zewnętrznego kolektora Syslog.**Monitorowanie infrastruktury (bezagentowo)** musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VolP i firewalle co najmniej w następującym zakresie:1. wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-pinq;
2. wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU);
3. wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci;
4. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła;
5. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku;
6. wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze;
7. wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie;
8. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny;
9. zablokowania mapy urządzeń przed przypadkową edycją;
10. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów – program musi monitorować czas ich odpowiedzi i procent utraconych pakietów;
11. serwerów pocztowych:
12. program musi monitorować czas logowania do serwisu odbierającego oraz czas wysyłania poczty,
13. program mus mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i innych), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
14. program musi mieć możliwość wykonywania operacji testowych,
15. program musi mieć możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.
16. monitorowania serwerów WWW i adresów URL;
17. cykliczneqo monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS;
18. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail;
19. obsługi urządzeń SNMP wspierających SNMP v 1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VolP itp.) - monitorowanie wartości za pomocą nazw zmiennych oraz OID.
20. obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych;
21. monitoringu routerów i przełączników wg:
22. zmian stanu interfejsów sieciowych;
23. ruchu sieciowego;
24. podłączonych stacji roboczych - graficzna prezentacja panelu switcha;
25. ruchu generowanego przez podłączone do portów stacje robocze;
26. serwisów Windows: monitor serwisów Windows musi alarmować gdy serwis przestanie działać oraz musi pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie;
27. wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu;
28. wydajności systemów Windows:
29. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Program musi posiadać funkcjonalność opartą na inteligentnych mapach i oddziałach, które służą do lepszego zarządzania logiczną strukturą urządzeń w urzędzie (oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (mapy Inteligentne). Program musi posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.Program musi umożliwiać również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów, definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy muszą być budowane przez administratora z wykorzystaniem ciągu przyczynowo skutkowego - oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.Program musi nieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).**W zakresie inwentaryzacji** program musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Obejmować co najmniej zestawienie posiadanych konfiguracji sprzętowych, informację o wolnym miejscu na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
3. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
4. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
5. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
6. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
7. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
8. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
9. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (dłuqość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
10. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania co najmniej w następującym zakresie:1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
2. tworzenia powiązań między zasobami a urządzeniami;
3. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych;
4. wskazania osób uprawnionych do użycia zasobów;
5. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania musi istnieć możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (po podaniu daty, administrator może otrzymać powiadomienie e-mail np. o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz;
6. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów;
7. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów;
8. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie;
9. importu danych z zewnętrznego źródła (za pomocą plików \*.CSV);
10. przechowywania dowolnych dokumentów (np. pliki \*.DOCX, \*.XLSX, \*.PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.;
11. tworzenia powiązań między zasobami a dokumentami w relacji 1:N;
12. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.;
13. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
14. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
15. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo urzędu,
16. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
17. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
18. archiwizacji i porównywania audytów zasobów,
19. tworzenia kodów kreskowych dla zasobów,
20. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
21. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
22. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
23. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Wymagany jest agent inwentaryzacji działający co najmniej na systemie Android.Inwentaryzacja oprogramowania musi zapewnić funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP;
2. Informacje o aplikacjach używanych w organizacji;
3. Tworzenie własnych wzorców aplikacji;
4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.;
5. Informacje o komputerach, na których aplikacja została wykryta;
6. Zarządzanie posiadanymi licencjami;
7. Wskazywanie osób odpowiedzialnych za licencję;
8. Wskazanie użytkowników licencji;
9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N;
10. Rozbudowane zarzadzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu;
11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych;
12. Zarządzanie posiadanymi licencjami: raport zgodności licencji;
13. Możliwość przypisania do programów numerów seryjnych, wartości itp.;
14. Okna audytowe muszą posiadać możliwość filtrowania elementów per oddział.

**W zakresie obsługi użytkowników** program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:1. Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy);
2. Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach;
3. Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność;
4. Informacji o edytowanych przez użytkownika dokumentach;
5. Historii pracy (cykliczne zrzuty ekranowe);
6. Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt);
7. Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika);
8. Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program powinien mieć możliwość monitorowania kosztów wydruków,
9. Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto musi mieć możliwość:1. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków - zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen powinny być tworzone dla użytkownika lub grupy użytkowników i powinny być kopiowane pomiędzy grupami lub kontami;
2. Blokowania ruchu na wskazanych portach TCP/IP;
3. Blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
4. Wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia;
5. Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika);
6. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Wymagana możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.Wymagany mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji powinny być tworzone dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.Program musi posiadać tworzenie grupy użytkowników oraz grup Inteligentnych, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.**Zdalna pomoc użytkownikom.** W ramach kontroli stacji użytkownika musi być dostępny podgląd pulpitu użytkownika i musi istnieć możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu musi mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W wymaganym module powinna się znajdować baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Moduł musi umożliwiać przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. W ramach funkcjonalności modułu wymagane jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł musi zawierać komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadania artykułom jednego z trzech statusów (opublikowany, wewnętrzny, szkic). Program musi umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Dostęp do systemu zgłoszeń oraz bazy wiedzy musi być realizowany przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.Funkcjonalność modułu musi umożliwiać uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.Moduł pomocy zdalnej musi umożliwiać również:1. Pobieranie listy użytkowników z usługi katalogowej np. Active Directory;
2. Zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont;
3. Zarzadzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarzadzania regułami widoczności zgłoszeń;
4. Zarządzanie dostępem do czatu w trzech poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej;
5. Tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do czterech poziomów kategorii), opisami kategorii oraz klauzulą RODO;
6. Automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
7. Procesowanie zgłoszeń użytkowników z wiadomości e-mail;
8. Tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń;
9. Wykonywanie operacji na wielu zgłoszeniach równocześnie;
10. Dołączanie załączników do zgłoszeń;
11. Rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy;
12. Szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników;
13. Wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia;
14. Zrzuty ekranowe (podgląd pulpitu);
15. Dystrybucję oprogramowania przez Agenty;
16. Dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI);
17. Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku;
18. Możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu;
19. Planowanie nieobecności pracowników helpdesk;
20. Obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem;
21. Generowanie raportów obsługi helpdesk;
22. Zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu);
23. Zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami);
24. Wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

Wymagana funkcjonalność **ochrony danych przed wyciekiem** poprzez blokowanie urządzeń w następującym zakresie.1. Blokowanie urządzeń i nośników danych - program musi mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
9. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Wymagane jest zarządzanie prawami dostępu do urządzeń w następującym zakresie:1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików;
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. urządzenia prywatne są blokowane;
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników;
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci;
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane;

Wymagany audyt operacji na plikach na urządzeniach przenośnych:1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego.

Wymagane monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.Program musi wspierać zarządzanie czasem i analizować aktywność użytkowników poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji powinien mieć możliwość oznaczenia sesji aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Musi być również zapewniony dostęp do własnych wskaźników aktywności w czasie pracy. Przełożeni muszą mieć zapewnioną funkcjonalność polegającą na uzyskaniu automatycznego dostępu do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Wymagany jest dostęp przez przeglądarkę internetową, w której strona może być wyświetlana w trybie jasnym lub ciemnym. Funkcjonalności muszą zostać zapewnione poprzez dostarczenie co najmniej następujących informacji.1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
2. Statystyki aktywności grupy i jej członków widoczne dla przełożonego.
3. Statystyki aktywności podwładnych widoczne dla przełożonego.
4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji Globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
11. Wskaźnik czasu poświęconego na aktywność produktywną.
12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka predefiniowana lista kategorii z możliwością edycji.
14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

W ramach dostawy oprogramowania wymagane jest dostarczenie portalu informacyjnego w formie platformy WWW, która pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety powinny być rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych powinna być automatycznie odświeżana oraz może być:1. Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.
2. Wyświetlana w trybie jasnym lub nocnym.

Oprogramowanie musi umożliwiać zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.Widgety powinny prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania, co najmniej w następujących obszarach:1. Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci;
2. Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów;
3. Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW;
4. Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie;
5. Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), Produktywność dla grupy, Statystyki czasu nieproduktywnego.

Ochrona przed usunięciemProgram musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.Funkcjonalność AgentaMożliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze. |

|  |
| --- |
| 1. **Wymagania minimalne dla rozbudowa zabezpieczeń logicznych (firewall, IDS, IPS)**
 |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Typ** | W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia (rozwiązania). |
| **Wymagania ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 musi wspierać 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 - musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
 |
| **Interfejsy, Zasilanie:** | 1. System realizujący funkcję Firewall musi dysponować minimum:
* 10 portami Gigabit Ethernet RJ-45.
* 2 gniazdami SFP 1 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.
 |
| **Parametry wydajnościowe** | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
 |
| **Funkcje Systemu Bezpieczeństwa** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Zamawiający dopuszcza aby były one 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 - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
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. W ramach postępowania powinny zostać dostarczone 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. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
 |
| **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. Element systemu realizujący funkcję Firewall musi integrować 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
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
 |
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* 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.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać 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 musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
 |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
 |
| **Funkcje SD-WAN** | 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
 |
| **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
 |
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
 |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
 |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
 |
| **Kontrola www** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL.
5. Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
 |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać 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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
 |
| **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach dostawy musi zostać zapewnionyu (dostarczony) komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów.

Zamawiający wymaga zapewnienia tej funkcjonalności przez okres jednego roku, w okresie realizacji projektu, tj. nie dłużej niż do 30.09.2023 r. 1. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.
 |
| **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:* ICSA lub EAL4 dla funkcji Firewall.
 |
| **Serwisy i licencje** | W ramach realizacji zadania Zamawiający wymaga dostarczenia licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Zamawiający wymaga zapewnienia tej funkcjonalności przez okres jednego roku, w okresie realizacji projektu, tj. nie dłużej niż do 30.09.2023 r.Powinny one obejmować:* 1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen
	2. Licencja na usługę realizowaną w chmurze umożliwiająca logowanie i raportowanie z czasem retencji logów.
 |
| **Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 1 roku (12 miesięcy), polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| **Wymagania ogólne** | 1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
 |

|  |
| --- |
| 1. **Wymagania minimalne dla diagnozy cyberbezpieczeństwa**
 |
| 1. W ramach przedmiotu zamówienia należy wykonać diagnozę cyberbezpieczeństwa zgodnie z wymaganiami programu “Cyfrowa Gmina” oraz obowiązującymi przepisami prawa w tym zakresie.
2. Szczegółowy zakres przedmiotu diagnozy zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 8 Regulaminu Konkursu Grantowego Cyfrowa Gmina.
3. Regulamin Konkursu Grantowego Cyfrowa Gmina wraz z formularzem - załącznikiem nr 8 został zamieszczony na stronie Centrum Projektów Polska Cyfrowa pod adresem https://www.gov.pl/web/cppc/cyfrowa-gmina.
4. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz Rozporządzeniem 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 (zwane Rozporządzeniem KRI).
5. Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu:
6. Certified Internal Auditor (CIA)
7. Certified Information System Auditor (CISA)
8. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018r. poz. 650 i 1138 ), w zakresie certyfikacji osób;
9. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
10. Certified Information Security Manager (CISM);
11. Certified in Risk and Information Systems Control (CRISC);
12. Certified in the Governance of Enterprise IT (CGEIT);
13. Certified Information Systems Security Professional (CISSP);
14. Systems Security Certified Practitioner(SSCP);
15. Certified Reliability Professional;
16. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.
17. Dokument końcowy musi być podpisany przez osobę posiadającą uprawnienia (wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu) raport oraz wypełniony formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa (załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina) należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.

Zamawiający wymaga przeprowadzenia wszystkich czynności (poza sporządzeniem raportu) objętych diagnozą cyberbezpieczeństwa (audytem) w sposób stacjonarny, tj. w miejscu świadczenia usługi w siedzibie Zamawiającego w Urzędzie Gminy w Wiązownicy. Diagnoza musi zostać przeprowadzona w maksymalnym stopniu obiektywnie - poprzez przeprowadzone badania w Urzędzie w celu przedstawienia rzeczywistego stanu cyberbezpieczeństwa Urzędu. Zamawiający zakłada, że Wykonawca przeznaczy nie mniej niż 3 dni roboczych na wykonanie diagnozy (audytu) z tego minimum 1 dzień spędzi w Urzędzie na prowadzenie analiz do audytu w kontakcie z wskazanymi przez Zamawiającego pracownikami urzędu. |

# WARUNKI URUCHOMIENIA I ODBIORU WDROŻONYCH ROZWIĄZAŃ ORAZ PRZEKAZANIA DO EKSPLOATACJI

* 1. **Pozostałe wymagania stawiane Wykonawcom**

Poza dostawami i usługami podstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii, uwzględniając warunki ich wykonania. Wykonawca musi ponadto uwzględnić w cenie w ramach kosztów dodatkowych:

1. koszty zabezpieczenia istniejących elementów obiektuoraz wyposażenia (urządzeń) Zamawiajacego przed ich zniszczeniem w trakcie wykonywania prac,
2. koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego
3. koszty zapewnienia bezpieczeństwa bhp i ppoż. w trakcie realizacji prac
4. koszty testów, prób, badań, odbiorów technicznych – jeśli są wymagane
	1. **Stosowanie rozwiązań z zakresu interoperacyjności**

Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności mi. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowania minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega mi. na:

1. zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa
2. redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych
3. zapewnienia bezpieczeństwa plików
4. dbałość o aktualizację oprogramowania

Dodatkowym ważnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń).

Konieczność zapewnienia tej funkcjonalności wynika z:

1. §21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej)
2. Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa

**Wdrożone rozwiązania powinny spełniając wymagania przywołanych aktów prawnych oraz standardów rynkowych.**

* 1. **Dokumenty odbioru końcowego**
1. Protokoły odbiorów częściowych
2. Protokoły z pomiarów i testów - jeśli dotyczy
3. Odpowiednie atesty i certyfikaty - jeśli są wymagane
4. Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta