



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

## Szczegółowy Opis Przedmiotu Zamówienia

na dostawę sprzętu i oprogramowania informatycznego oraz usługi związane  
z realizacją projektu „Cyberbezpieczny Samorząd” dla jednostek  
organizacyjnych Gminy Sulechów



Cyberbezpieczny  
Samorząd

## Spis treści

1. Zestawienie ilościowe.....	3
2. Zasada równoważności rozwiązań i neutralności technologicznej. ....	4
3. Przedmiot zamówienia dla części nr 1.....	6
3.1. Wymagania ogólne.....	6
3.2. Zakup NAS (1 szt.).....	9
3.3. Zakup serwera (1 szt.). ....	10
3.4. Zakup firewall (1 szt.). ....	12
3.5. Zakup przełącznika (1 szt.).....	15
3.6. Zakup oprogramowania backup (1 szt.). ....	16
4. Opis przedmiotu zamówienia części nr 2. ....	20
4.1. Wymagania ogólne.....	20
4.2. Zakup oprogramowania antywirusowego (2 szt.). ....	23
4.3. Zakup oprogramowania do zarządzania bezpieczeństwem IT (1 szt.). ....	29
4.4. Zakup serwerowego systemu operacyjnego dla VM zarządzania bezpieczeństwem IT. ....	32

## 1. Zestawienie ilościowe.

Część nr 1 – Dostawa sprzętu i oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Zakup NAS	1 szt.
2.	Zakup serwera	1 szt.
3.	Zakup firewall	1 szt.
4.	Zakup przełącznika	1 szt.
5.	Zakup oprogramowania backup	1 szt.

Część nr 2 – Dostawa oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Zakup oprogramowania antywirusowego	2 szt.
2.	Zakup oprogramowania do zarządzania bezpieczeństwem IT	1 szt.
3.	Zakup serwerowego systemu operacyjnego dla VM zarządzania bezpieczeństwem IT	1 szt.

## 2. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe

wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

### 3. Przedmiot zamówienia dla części nr 1.

#### 3.1. Wymagania ogólne.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów. Niedopuszczalna jest realizacja tylko części funkcji bądź wymaganych standardów zamiast innych określonych jako minimalne w niniejszym dokumencie. Wszystkie wymagania minimalne muszą zostać zapewnione przez dostarczane produkty bez konieczności zakupu żadnych dodatkowych elementów przez Zamawiającego, chyba że z niniejszego dokumentu wynika inaczej.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji przez Zamawiającego, będą to następujące lokalizacje:
  - a. Centrum Usług Wspólnych w Sulechowie (dalej w skrócie: CUW), ul. Licealna 18A, 66-100 Sulechów (serwer, firewall, przełącznik);
  - b. Ośrodek Pomocy Społecznej w Sulechowie (dalej w skrócie: OPS), ul. Jana Pawła II-go 52, 66-100 Sulechów;
  - c. Urząd Miejski Sulechów (dalej w skrócie: urząd), Plac Ratuszowy 6, 66-100 Sulechów (NAS dla OPS, który będzie zlokalizowany w serwerowni urzędu).
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania, w tym minimum:
  - a. Dla NAS w OPS, Wykonawca jest zobowiązany uruchomić NAS w siedzibie urzędu wraz z jego konfiguracją, skonfigurować połączenie VPN pomiędzy OPS a urzędem na potrzeby komunikacji NAS. Wykonawca jest zobowiązany podpiąć zasoby tego NAS jako magazyn na backupy off-site systemu Veeam Backup pracującego w OPS, przez dodanie odpowiednich zadań do harmonogramu backupów,
  - b. Serwer w CUW ma pełnić rolę serwera do backup – Wykonawca jest zobowiązany zainstalować na nim system operacyjny i oferowany przez Wykonawcę program do backupu, a następnie

- skonfigurować program do backupu podpinając istniejące w CUW serwery jako źródło danych do backupowania,
- c. W ramach realizacji przedmiotu zamówienia dla CUW Wykonawca jest zobowiązany podłączyć urządzenia UTM oraz przełączniki, ustawić reguły filtrowania ruchu na UTM, ustawić połączenia VPN itp., skonfigurować przełącznik w, w tym ustawiać VLANy,
  - d. Inne, niezbędne prace w celu uruchomienia urządzeń zgodnie z zaleceniami Zamawiającego.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
12. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia sprzętu i oprogramowania – wymagania minimalne:
- a. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego sprzętu i oprogramowania po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniającą obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
    - i. scenariusze testowe, procedury oraz wzory raportów testów,
    - ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
    - iii. opis koncepcji realizacji prac,
    - iv. zalecenia przedwdrożeńowe dla Zamawiającego, jeżeli będą wymagane.
  - b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
    - i. Wykonawca prześle do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni kalendarzowych od dnia zawarcia umowy,

- ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
  - iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
  - iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
  - v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
  - vi. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
- c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
  - d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
  - e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
  - f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
13. Instruktaże w zakresie dostarczonego sprzętu i oprogramowania – wymagania minimalne.
- a. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
  - b. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
  - c. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 3 osoby).
  - d. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
  - e. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.
14. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.



### 3.2. Zakup NAS (1 szt.).

Minimalne parametry urządzenia:

1. Obudowa do szafy RACK.
2. Procesor wielordzeniowy osiągający w teście wydajności PassMark Performance Test co najmniej wynik 8 500 punktów, testy powinny być aktualne w okresie nie dłuższym niż 30 dni przed składaniem ofert. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności.
3. Pamięć RAM: min. 32 GB.
4. Pamięć flash: min. 4 GB.
5. Funkcje: wsparcie dla wirtualizacji, scentralizowana pamięć masowa na dane, backup, udostępnianie i przywracanie systemu po awarii.
6. Możliwość zainstalowania łącznie 8 dysków 3,5 calowych, min. SATA 3 - 6 Gb/s.
7. Zainstalowane dyski: min. 8 x dysk 8 TB SATA 6 GB/s przeznaczonych dla systemów NAS pracujących w trybie ciągłym. dyski muszą być zgodne z urządzeniem NAS, tj. muszą znajdować się na liście zgodności prowadzonej przez producenta urządzenia NAS lub które zostały przetestowane pod kątem zgodności z produktami producenta urządzenia NAS.
8. Poziom RAID: 1,5,6.
9. Kompatybilność dysków: 3,5-calowe dyski twarde SATA; 2,5-calowe dyski twarde SATA; 2,5-calowe dyski SSD SATA.
10. Obsługa połączeń 10GbE SFP+ (co najmniej dwa porty) oraz 10 GbE RJ45 (co najmniej dwa porty) wraz z 2 wkładkami 10GbE SFP+ do NAS oraz niezbędnymi kablami do połączenia NAS z przełącznikiem za pomocą wszystkich interfejsów.
11. Porty USB: min. 2x USB 3.0.
12. Szyny do montażu w szafie RACK.
13. Dostawa oprogramowania do archiwizacji m.in. maszyn wirtualnych Hyper-V z możliwością automatycznego odtworzenia całej maszyny wirtualnej z kopii oraz z kopii już obecnie posiadanych maszyn wirtualnych.
14. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany NAS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta NAS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany NAS wymagań w zakresie określonym powyżej.
15. Gwarancja producenta min. 24 miesiące realizowanej w miejscu instalacji sprzętu, z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia. Gwarancja musi obejmować także dyski. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.

### 3.3. Zakup serwera (1 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 3.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowany jeden procesor klasy x86 dedykowany do pracy z oferowanym serwerem, umożliwiający osiągnięcie przez serwer wyniku co najmniej 145 punktów w teście SPECrate2017\_fp\_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie [www.spec.org](http://www.spec.org). Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 64 GB w najnowszej technologii oferowanej przez producenta, płyta główna musi obsługiwać do min. 1 TB pamięci RAM DDR5.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC i/lub Demand Scrubbing i/lub Patrol Scrubbing i/lub Permanent Fault Detection (PFD).
6. Zintegrowana karta graficzna ze złączem VGA.
7. Interfejsy sieciowe: Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz co najmniej 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 6 dysków twardych Hot-Plug NL SAS o prędkości min. 12 Gb/s o pojemności co najmniej 8 TB każdy oraz co najmniej 2 dyski twarde Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 960 GB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Możliwość zainstalowania co najmniej dwóch dysków M.2 SATA z możliwością konfiguracji RAID 1.
10. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
11. Wsparcie dla dysków samoszyfrujących.
12. Wbudowane porty: min. 3 porty USB, w tym co najmniej 1 port USB musi być dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
13. Wentylatory: Redundantne typu Hot Plug.
14. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 1100 W każdy.
15. Karta/moduł zarządzania: Niezależny od zainstalowanego na serwerze systemu operacyjnego posiadający dedykowane złącze umożliwiający:
  - 1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
  - 2) zdalne monitorowanie i informowanie o statusie serwera,
  - 3) szyfrowane połączenie oraz autentykację i autoryzację użytkownika,
  - 4) możliwość podmontowania zdalnych wirtualnych napędów,
  - 5) wirtualną konsolę z dostępem do myszy, klawiatury,

- 6) wsparcie dla IPv6,
  - 7) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
  - 8) integracja z Active Directory,
  - 9) wsparcie dla dynamic DNS.
16. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
- 1) wbudowane diody informacyjne lub wyświetlacz informujący o stanie serwera;
  - 2) blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
  - 3) moduł TPM 2.0.
17. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzanie serwerem klasy Microsoft Windows Server Standard 2025 wraz z 5 licencjami dostępowymi umożliwiającymi korzystanie przez 5 urządzeń z zasobów serwera lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.
- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Server Standard 2025 wraz z 5 licencjami dostępowymi Microsoft Windows Server 2025 CAL Device:
- 1) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego dla minimum 5 urządzeń.
  - 2) Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
  - 3) 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.
  - 4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
  - 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
  - 6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
  - 7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
  - 8) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
  - 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 zaporą internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
  - 14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

- 15) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
  - 16) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
  - 17) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
  - 18) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
  - 19) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
  - 20) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
18. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
19. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływ na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów w zakresie określonym powyżej.
20. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia.

### 3.4. Zakup firewall (1 szt.).

W ramach działania przewiduje się zakup urządzenia UTM wraz z licencjami subskrypcyjnymi. Subskrypcja musi umożliwić Zamawiającemu korzystanie z aktualnych baz funkcji ochronnych producenta i serwisów oraz obejmować firewall, IPS, kształtowanie pasma, antywirus, antyspam, web filtering. W ramach przedmiotu zamówienia Wykonawca musi zapewnić także wsparcie techniczne, które może być tylko realizowane przez producenta, dystrybutora, bądź oficjalnego partnera dystrybutora. Subskrypcja dla urządzenia UTM obejmująca wszystkie wymagania wskazane powyżej musi być dostarczona na okres do dnia 26.03.2026 r. niezależnie od oferowanych modeli licencjonowania producenta.

#### Minimalne wymagania techniczne urządzenia:

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych.
2. System musi wspierać IPv4 oraz IPv6 w zakresie minimum: firewall, ochrony IPS oraz usług sieciowych.
3. Interfejsy: liczba portów Ethernet 2,5 Gbps – min. 8; liczba portów światłowodowych 1 Gbps – min. 1; urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
4. Wydajność:
  - Przepustowość firewall – co najmniej 8 Gbps,
  - Liczba równoległych sesji – co najmniej 0,4 mln,
  - Przepustowość IPS – co najmniej 4 Gbps,
  - Liczba jednoczesnych klientów SSL VPN – co najmniej 100.
5. Funkcje Systemu Bezpieczeństwa dostępne w ramach dostarczonej licencji:
  - Komercyjny antywirus,
  - Firewall,
  - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,
  - Ochrona przed atakami - Intrusion Prevention System,
  - Kontrola stron WWW,
  - Kontrola zawartości poczty – Antyspam,
  - Zarządzanie pasmem (Traffic shaping),
  - Analiza ruchu szyfrowanego protokołem SSL.
6. Polityki firewall:
  - Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, IPS i aplikacje, reakcje zabezpieczeń, rejestrowanie zdarzeń,
  - System musi zapewniać translację adresów NAT oraz PAT,
7. Połączenia VPN:
  - System musi umożliwiać konfigurację połączeń typu IPSec VPN,
  - System musi umożliwiać konfigurację połączeń typu SSL VPN.
8. Routing i obsługa łączy WAN:
  - W zakresie routingu rozwiązanie powinno zapewniać obsługę: routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu,
  - System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia.
9. Kontrola antywirusowa:
  - Urządzenie musi umożliwiać zastosowanie skanera antywirusowego, który musi zostać dostarczony w ramach podstawowej licencji,
  - Administrator musi mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym,
  - Administrator musi mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji.

#### 10. Ochrona przed atakami:

- Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS,
- Moduł IPS musi nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia,
- Urządzenie musi umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS,
- Administrator musi mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP,
- Urządzenie musi umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0,
- Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

#### 11. Kontrola WWW:

- Urządzenie musi posiadać wbudowany filtr URL,
- Filtr URL musi działać w oparciu o klasyfikację URL,
- Administrator musi mieć możliwość dodawania własnych kategorii URL,
- Administrator musi mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru musi być przynajmniej:
  - i. blokowanie dostępu do adresu URL,
  - ii. zezwolenie na dostęp do adresu URL,
  - iii. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora,
- Administrator musi mieć możliwość skonfigurowania stron z komunikatem o zablokowaniu strony,
- Filtr URL musi uwzględniać komunikację po protokole HTTPS,
- Urządzenie musi umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane,
- Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania.

#### 12. Uwierzytelnianie użytkowników w ramach sesji:

- System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą co najmniej haseł statycznych,
- Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.

#### 13. Zarządzanie:

- Konfiguracja urządzenia musi być możliwa z wykorzystaniem polskiego interfejsu graficznego,
- Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS,
- Urządzenie musi umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami,
- Urządzenie musi umożliwiać zarządzanie z poziomu konsoli (SSH),

- Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup,
  - Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników,
  - Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog),
  - Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa),
14. Urządzenie powinno umożliwiać monitorowanie logów ruchu, administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania, rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail, urządzenie powinno mieć możliwość generowania raportów.
  15. Urządzenie musi posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
  16. W ramach Zamówienia Wykonawca dostarczy licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować firewall, IPS, kształtowanie pasma, antywirus, antyspam, web filtering na okres do dnia 26.03.2026 r.
  17. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany firewall spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta firewall lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany firewall wymagań w zakresie określonym powyżej.
  18. Urządzenie musi być objęte serwisem gwarancyjnym producenta na okres do dnia 26.03.2026 r. obejmującym w przypadku zgłoszenia awarii urządzenia, wysyłkę urządzenia zastępczego lub wysyłkę sprawnego urządzenia w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana musi zostać na kolejny dzień roboczy.

### 3.5. Zakup przełącznika (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzalny przełącznik L2+.
2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).
3. Przepustowość routowania/przełączania: min. 170 Gbit/s.
4. Prędkość przekazywania: min. 130 Mpps.
5. Bufor pamięci dla pakietów: max. 3 MB.
6. Rozmiar tablicy MAC: min. 16 000 wpisów.
7. Dostępne interfejsy: min. 48 x 1000Base-T- RJ-45 PoE+, min. 4 x 10GbE SFP+.
8. Obsługiwane standardy komunikacyjne: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.3ab, IEEE 802.3ae, IEEE 802.3af, IEEE 802.3at, IEEE 802.3i, IEEE 802.3u, IEEE 802.3z.
9. Obsługiwane protokoły zarządzające: SNMPv1, SNMPv2, SNMPv3, RMON.
10. Obsługiwane protokoły sieciowe: IPv4, IPv6, LLDP, MSTP, RSTP, Telnet, TACACS, MLD, SSH.

11. Inne cechy: zarządzanie przez www, generowanie raportów zdarzeń systemowych, obsługa min. 250 sieci VLAN, obsługa multicast, uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia; obsługa list kontroli dostępu (ACL).
12. Możliwość łączenia urządzeń w stos min. 4.
13. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik sieciowy spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta przełącznika sieciowego lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik wymagań w zakresie określonym powyżej.
14. Co najmniej 24 miesiące gwarancji producenta.

### 3.6. Zakup oprogramowania backup (1 szt.).

Minimalne wymagania oprogramowania backup:

1. System powinien umożliwiać tworzenie kopii zapasowych Centrum Usług Wspólnych dla 3 serwerów fizycznych oraz 8 maszyn wirtualnych.
2. System musi tworzyć „samowystarczalne” archiwa do odzyskania których nie jest wymagana osobna baza danych.
3. System musi mieć mechanizmy kompresji w celu zmniejszenia wielkości archiwów.
4. System musi zapewniać backup jednoprzebiegowy.
5. System musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania.
6. System musi mieć możliwość uruchamiania skryptów przed i po zadaniu backupowym.
7. System musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
8. System musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej.
9. System musi wspierać backup maszyn wirtualnych.
10. System powinien zapewniać wykonywanie kopii zapasowych plików przechowywanych na urządzeniach pracujących pod kontrolą systemów Windows i Linux.
11. System powinien mieć możliwość pracy w programie z dowolnego miejsca bez potrzeby korzystania z Pulpitu zdalnego, jednoczesnej pracy z danym serwerem przez kilku administratorów.
12. System powinien mieć wbudowane następujące funkcje:
  - a. Możliwość wykonania backupu całego systemu operacyjnego, łącznie z zainstalowanymi programami, sterownikami i danymi użytkownika, tak aby w przypadku awarii możliwe było odzyskanie działającego systemu operacyjnego i wszystkich zainstalowanych komponentów.
  - b. Zautomatyzowane przywracanie systemu operacyjnego z serwerów (prosty sposób przywracania systemu operacyjnego z serwera kopii zapasowych poprzez sieć do uszkodzonego komputera). Możliwość przywrócenia po awarii systemu operacyjnego wraz z



wszystkimi zainstalowanymi programami (ang. bare-metal restore), tak aby uruchomić system operacyjny bez potrzeby ponownej instalacji i konfiguracji.

- c. Ochrona przed programami ransomware szyfrującymi pliki.
- d. Backup i odzyskiwanie maszyn wirtualnych Hyper-V oraz VMWare ESX, ESXi. Program powinien wykonywać kopie zapasowe zarówno zatrzymanych jak i uruchomionych maszyn wirtualnych.
- e. Certyfikaty SSL dla połączeń HTTPS – możliwość obsługi samopodpisanych certyfikatów oraz stosowania własnych certyfikatów SSL.
- f. Zabezpieczanie połączeń sieciowych w systemach archiwizacji danych - typu klient-serwer za pomocą reguł IPsec.
- g. Możliwość archiwizacji danych w chmurze.
- h. Backup plików PST (MS Outlook) - backup plików PST bez zamykania programu Outlook.
- i. Możliwość automatycznego backupu urządzenia przy zamykaniu systemu.
- j. Archiwizacja danych także na napędy taśmowe – możliwość replikacji na napędy taśmowe.
- k. Możliwość backupu na dysk sieciowy - składowanie kopii na urządzeniach typu NAS szybkim i wydajnym protokołem iSCSI.
- l. Możliwość instalacji serwera backupu pod systemem Linux i Mac OS.
- m. Możliwość wydajnego i pewnego backupu baz danych i plików poczty (Microsoft SQL Server, Microsoft Exchange Server, Oracle, MySQL, InterBase, Firebird, Microsoft Access, dBase, Paradox oraz plików programów pocztowych: Microsoft Outlook, Outlook Express, Mozilla Thunderbird).
- n. Możliwość archiwizacji otwartych i zablokowanych plików.
- o. Możliwość szyfrowania archiwów (w tym AES 256).
- p. Możliwość wykonywania archiwizacji pełnej i różnicowej, także różnicowej na poziomie fragmentów plików (archiwizowane są tylko te części plików, które zostały zmodyfikowane od czasu poprzednich archiwizacji a pozostałe są pomijane).
- q. Możliwość generowania raportów i statystyk, które pomagają w analizie działania aplikacji (Raporty informujące o niewykonanych i opóźnionych zadaniach archiwizacji i statystyki zawierające informacje na temat szybkości i rozmiaru backupu z poszczególnych komputerów).
- r. Możliwość wykonywania zadań archiwizacji w/g harmonogramu następującego typu: Na żądanie - zadanie archiwizacji będzie wykonywane tylko przez manualne uruchomienie zadania; Codziennie - zadanie archiwizacji będzie uruchamiane codziennie o wskazanej godzinie; Co określoną liczbę dni - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę dni; Co określoną liczbę godzin - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę godzin; Co określoną liczbę minut - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę minut; W dni tygodnia - zadanie archiwizacji będzie wykonywane automatycznie w wybrane dni tygodnia; Czas rozpoczęcia - umożliwia ustalenie terminu rozpoczęcia zadania archiwizacji z dokładnością do jednej minuty; Następny termin - umożliwia ustalenie daty kolejnej archiwizacji; Zadania opóźnione mogą być pominięte i wykonane w następnym terminie, wykonane natychmiast po podłączeniu serwera; Przy zamykaniu systemu.
- s. Dziennik zdarzeń służący do sprawdzania poprawności działania systemu i wyszukiwania przyczyn ewentualnych problemów – możliwość na bieżąco śledzenia generowanych zdarzeń, dotyczących działania całego systemu, takie jak: błędy, ostrzeżenia i informacje.

Wszystkie zapisane zdarzenia można filtrować co najmniej według typu zdarzenia oraz nazwy komputera, którego dana informacja dotyczy.

- t. Podczas wyboru plików i katalogów do archiwizacji pozwalać określić woluminy, maski lub pełne ścieżki do plików i katalogów, które mają być archiwizowane i te, które mają być wykluczone z archiwizacji.
  - u. Obsługę co najmniej następujących rodzajów archiwizacji: archiwizacja pełna; archiwizacja różnicowa; archiwizacja różnicowa na poziomie fragmentów plików.
  - v. Obsługę kopii rotacyjnych (wersjonowanie, retencja danych - pozwala określić, ile maksymalnie przechowywać archiwów na dysku, ile przechowywać kopii wstecz).
  - w. Obsługę replikacji archiwów - archiwa należące do wybranego zadania backupu mogą być powielane w inne miejsce, replikacja może być wykonywana na napędy dyskowe, optyczne i taśmowe.
  - x. Monitoring i kontrola pracy serwera backupu, powinna w łatwy i intuicyjny sposób umożliwić zatrzymanie i uruchomienie serwera backupu, możliwość wywołania wirtualnego wiersz poleceń na serwerze backupu i podłączonych stacjach roboczych.
  - y. Dziennik zdarzeń służy do sprawdzania poprawności działania Systemu i wyszukiwania przyczyn ewentualnych problemów. W zakładce Dziennik zdarzeń można na bieżąco śledzić wszystkie generowane zdarzenia dotyczące działania całego Systemu (serwera jak i stacji roboczych), takie jak: błędy, ostrzeżenia i informacje.
  - z. Wszystkie zapisane zdarzenia można filtrować według typu zdarzenia oraz nazwy urządzenia, którego dana informacja dotyczy.
  - aa. Wysyłanie alertów administracyjnych, zawierających raporty lub wybrane komunikaty z dziennika zdarzeń, wg ustalonego harmonogramu na wskazany adres e-mail lub np. do serwera syslog.
  - bb. Możliwy dostęp do zasobów sieciowych przez np. definiowanie ścieżki UNC, dyski sieciowe i dyski serwerów FTP, które mogą być wykorzystywane przez system jako: miejsce przechowywania archiwów, katalog docelowy replikacji, ścieżka zapisu alertów administracyjnych.
  - cc. Możliwe używania poleceń lokalnych, służących do rozszerzania funkcjonalności programu. Dzięki nim można automatycznie uruchamiać na serwerze backupu zewnętrzne programy, skrypty lub pliki wsadowe, wykonywać operacje na plikach, wykorzystywać komponenty ActiveX, sterować usługami Active Directory, itp.
  - dd. Program może być uruchamiany w trybie Usługi systemowej lub awaryjnie, także w trybie aplikacji użytkownika.
  - ee. Możliwe uruchomienie programu w trybie diagnostycznym oraz w trybie naprawy bazy danych.
13. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania w formie licencji czasowych lub subskrypcyjnych:
- a. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 26.03.2026 r.
  - b. Pomimo możliwości ograniczenia czasowego udzielenia gwarancji na oferowane oprogramowanie, sama licencja nie może czasowo ograniczać funkcjonalności oprogramowania (musi być bezterminowa), a jedynie po wygaśnięciu okresu gwarancji licencja może ograniczyć dostęp do nowych aktualizacji i innych funkcjonalności związanych z gwarancją i serwisem.

- c. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
- d. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 26.03.2026 r.
- e. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
  - i. dostęp do najnowszych wersji oprogramowania,
  - ii. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
  - iii. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
  - iv. przyjmowanie i realizacja zgłoszeń serwisowych,
  - v. doradztwo techniczne w zakresie konfiguracji i optymalizacji oprogramowania,

w przypadku jeżeli w dalszej części niniejszego dokumentu zdefiniowano wymogi serwisu lub gwarancji w innym zakresie powyższe wymogi są obowiązujące i należy potraktować jako podstawowe, precyzowane przez dodatkowe wymagania opisane w dalszej części dokumentu.

## 4. Opis przedmiotu zamówienia części nr 2.

### 4.1. Wymagania ogólne.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz nienoszące oznak użytkowania.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe, oprogramowanie nie może znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wykonawca zapewni dostawę oprogramowania do wskazanej lokalizacji przez Zamawiającego, będą to następujące lokalizacje:
  - a. Centrum Usług Wspólnych w Sulechowie (dalej w skrócie: CUW), ul. Licealna 18A, 66-100 Sulechów (serwer, firewall, przełącznik);
  - b. Ośrodek Pomocy Społecznej w Sulechowie (dalej w skrócie: OPS), ul. Jana Pawła II-go 52, 66-100 Sulechów;
5. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
6. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
7. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
8. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
  - a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego w siedzibie CUW i OPS, a w przypadku jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.

- b. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
  - c. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
  - d. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
  - e. Usługa wsparcia wdrożenia obejmuje:
    - i. przeprowadzenie analizy przedwdrożeniowej,
    - ii. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
    - iii. rejestracja produktu – jeżeli wymagana,
    - iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
    - v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
    - vi. konfigurację oprogramowania,
    - vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
    - viii. szkolenie administratorów z zakresu pracy z programem,
    - ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połączenie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.
9. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
- a. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
    - i. scenariusze testowe, procedury oraz wzory raportów testów,
    - ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
    - iii. opis koncepcji realizacji prac,
    - iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
  - b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
    - i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni roboczych od dnia zawarcia umowy,
    - ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
    - iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,

- iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
  - v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
  - vi. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
- c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
  - d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
  - e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
  - f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
10. Wymagania licencyjne dla dostarczonego oprogramowania:
- a. Licencjobiorcą licencji będą jednostki organizacyjne Gminy Sulechów, tj. dla Centrum Usług Wspólnych w Sulechowie oraz Ośrodka Pomocy Społecznej w Sulechowie zgodnie ze wskazaniem poniżej.
  - b. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.
  - c. Licencje muszą obowiązywać do dnia 26.03.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania.
  - d. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
  - e. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.
  - f. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
  - g. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
  - h. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.

- i. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym urządzeniu klienckim (licencja nie może być przypisana do komputera/urządzenia).
  - j. Licencja oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.
  - k. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.
11. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania w formie licencji czasowych lub subskrypcyjnych:
- a. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 26.03.2026 r.
  - b. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
  - c. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 26.03.2026 r.
  - d. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
    - i. dostęp do najnowszych wersji oprogramowania,
    - ii. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
    - iii. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
    - iv. przyjmowanie i realizacja zgłoszeń serwisowych,
    - v. doradztwo techniczne w zakresie konfiguracji i optymalizacji oprogramowania,w przypadku jeżeli w dalszej części niniejszego dokumentu zdefiniowano wymogi serwisu lub gwarancji w innym zakresie powyższe wymogi są obowiązujące i należy potraktować jako podstawowe, precyzowane przez dodatkowe wymagania opisane w dalszej części dokumentu.
12. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

#### 4.2. Zakup oprogramowania antywirusowego (2 szt.).

Oprogramowanie antywirusowe dla stacji roboczych musi stanowić jedno zintegrowane rozwiązanie, przez co Zamawiający rozumie minimum umożliwienie z poziomu administratora z poziomu jednej aplikacji w jednym interfejsie graficznym dostarczonego oprogramowania informowanie użytkownika/administratora o pojawiających się incydentach i zdarzeniach dotyczących np. próby ataku czy wykrycia złośliwego oprogramowania na poszczególnych hostach oraz inne wymogi funkcjonalne określone w wymaganiach poniżej. Wykonawca jest zobowiązany dostarczyć licencję dla Centrum Usług Wspólnych w Sulechowie umożliwiającą instalację na 40 urządzeń końcowych/użytkowników oraz Ośrodka Pomocy Społecznej w Sulechowie umożliwiającą instalację na 40 urządzeń końcowych/użytkowników (w sumie w ramach zadania należy dostarczyć 2 szt. oprogramowania antywirusowego - licencji, z czego każda na 40 urządzeń).

Oprogramowanie antywirusowe dla stacji roboczych powinno:

1. Umożliwiać centralną administrację.
2. Z poziomu centralnej administracji umożliwiać uruchomienie skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
3. Posiadać panel użytkownika/administratora systemu zlokalizowany w bezpiecznej chmurze producenta oprogramowania dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej.
4. Umożliwiać dostęp do panelu użytkownika poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów.
5. Prezentować parametry zasobów urządzeń/hostów aktualizowane w systemie na „żywo”, tj. w określonych interwałach czasowych, np. co minutę.
6. Używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.
7. Umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania.
8. Umożliwiać definiowanie złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców.
9. Umożliwiać wizualizację przy wykorzystaniu min. interaktywnych wykresów i grafik.
10. Posiadać wbudowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).
11. Umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS.
12. Umożliwiać użytkownikom generowanie raportów dotyczących wydajności i dostępności monitorowanych systemów.
13. Wykorzystywać szyfrowaną komunikację między agentami a serwerem.
14. Wykorzystywać agregację logów, która musi być oparta na technologii umożliwiającej indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym.
15. Umożliwiać gromadzenie danych z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).
16. Umożliwiać użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.
17. Posiadać interfejs użytkownika dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami, w tym standardy WCAG 2.1 na poziomie AA.
18. Rejestrować zdarzenia akcje i reakcje użytkowników z możliwością raportowania historii akcji poszczególnych użytkowników.

Minimalne wymagania oprogramowania dla stacji roboczych:

1. Ochrona antywirusowa powinna być zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp powinien być zapewniony przez przeglądarkę internetową.



2. Od strony chronionego środowiska nie może być wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy. Zamawiający zaleca, aby do prawidłowego działania wymagana była jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.
3. Rozwiązanie dla ochrony antywirusowej stacji roboczych wspierać powinno następujące systemy operacyjne: Microsoft Windows 10, Microsoft Windows 11, macOS 11 "Big Sur", macOS 10.15 "Catalina".
4. Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej to minimum: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari.
5. Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych powinno posiadać polski interfejs użytkownika.
6. Ochrona antywirusowa powinna być realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
7. Rozwiązanie posiadać powinno wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
8. Rozwiązanie wspierać powinno technologię Antimalware Scan Interface (AMSI).
9. Rozwiązanie umożliwiać powinno wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
10. W momencie wykrycia infekcji rozwiązanie automatycznie powinno podjąć próbę wyleczenia pliku, a jeśli nie jest to możliwe powinno przenosić go do bezpiecznego folderu kwarantanny.
11. Rozwiązanie posiadać powinno możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwalać powinno na minimum: wyleczeniu pliku, usunięciu, przeniesieniu do kwarantanny, zmiany nazwy, zablokowania.
12. Rozwiązanie posiadać powinno mechanizmy skanujące dyski sieciowe.
13. Skanowanie dysków sieciowych powinno być możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
14. Rozwiązanie posiadać powinno możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
15. Rozwiązanie musi posiadać mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
16. Rozwiązanie musi mieć możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
17. Aktualizacje baz definicji wirusów powinny być dostępne 24h na dobę na serwerze internetowym producenta.
18. Oprogramowanie musi umożliwiać aktualizację automatyczną oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
19. Oprogramowanie musi umożliwiać uaktualnienia definicji wirusów. Uaktualnienia definicji wirusów muszą posiadać podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
20. Oprogramowanie musi posiadać możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
21. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, musi następować w sposób automatyczny dla użytkownika końcowego.

22. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie powinno wymagać dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następować powinno automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
23. Oprogramowanie musi posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
24. Oprogramowanie musi posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
25. Oprogramowanie musi posiadać możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
26. Oprogramowanie musi posiadać możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
27. Oprogramowanie musi posiadać możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
28. Oprogramowanie musi posiadać możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
29. Skanowanie dysków przenośnych powinno móc odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.
30. Oprogramowanie musi umożliwiać przyrostowe pobieranie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy.
31. Oprogramowanie nie może wymagać restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
32. Oprogramowanie musi posiadać heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
33. Oprogramowanie musi umożliwiać wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
34. Oprogramowanie musi posiadać mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
35. Oprogramowanie musi posiadać technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
36. Oprogramowanie musi posiadać możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
37. Oprogramowanie musi posiadać możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
38. Oprogramowanie musi posiadać możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP, RAR, ARJ, LZH, TAR.
39. Oprogramowanie musi posiadać możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów powinien być możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
40. Oprogramowanie musi automatycznie powiadamiać użytkowników oraz administratora o pojawiających się zagrożeniach.

41. Oprogramowanie musi posiadać możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
42. Oprogramowanie musi posiadać możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
43. Oprogramowanie musi umożliwiać blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
44. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system producenta.
45. Oprogramowanie musi posiadać możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
46. Oprogramowanie musi być wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamianie skrypty ActiveX i pobierane pliki.
47. Oprogramowanie musi posiadać możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
48. Oprogramowanie musi umożliwiać blokowanie dostępu do kategorii witryn WWW skatalogowanych przez producenta oprogramowania.
49. Oprogramowanie powinno zapewniać kategoryzację klasyfikacji witryn WWW.
50. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, powinien zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
51. Oprogramowanie musi umożliwiać blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
52. Oprogramowanie musi posiadać wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” oprogramowanie powinno blokować możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
54. Kontrola połączenia umożliwiać powinna zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora.
55. Oprogramowanie musi posiadać wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
56. Oprogramowanie musi posiadać funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
57. Oprogramowanie musi pozwalać na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
58. Oprogramowanie musi posiadać możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
59. Oprogramowanie musi umożliwiać stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.

60. Oprogramowanie musi być wyposażone w mechanizm aktualizacji aplikacji umożliwiający instalację dostępnych poprawek dla systemu operacyjnego.
61. Administrator powinien posiadać możliwość uruchomienia aktualizacji dla systemu operacyjnego.
62. Mechanizm aktualizacji aplikacji musi umożliwiać automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
63. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego wymaga restartu hosta w celu jej zastosowania, administrator powinien posiadać możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
64. Oprogramowanie umożliwiać powinno blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
65. Oprogramowanie powinno posiadać opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
66. Oprogramowanie powinno uniemożliwiać zmiany w konfiguracji dokonywane przez użytkownika końcowego dla poszczególnych funkcji aplikacji wskazanych przez administratora.
67. Oprogramowanie powinno posiadać możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker.
68. Oprogramowanie powinno umożliwiać zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
69. Oprogramowanie powinno umożliwiać zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
70. Administrator w konsoli zarządzającej powinien posiadać dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
71. Oprogramowanie powinno posiadać wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
72. W przypadku wykrycia szkodliwego działania ransomware, moduł powinien blokować aktywność szkodliwego procesu oraz przywracać pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
73. Administrator powinien mieć możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
74. Administrator powinien mieć możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
75. Oprogramowanie powinno posiadać funkcjonalność kontroli uruchamianych aplikacji.
76. Tworzone reguły dotyczyć powinny minimum następujących czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
77. Oprogramowanie powinno pozwalać na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących minimum: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD).

### 4.3. Zakup oprogramowania do zarządzania bezpieczeństwem IT (1 szt.).

Przedmiotem zamówienia jest dostawa i wdrożenie oprogramowania do zarządzania bezpieczeństwem IT umożliwiającego szereg funkcji podnoszących cyberbezpieczeństwo w jednostce organizacyjnej Gminy Sulechów, tj. Ośrodka Pomocy Społecznej w Sulechowie (OPS) na maszynie wirtualnej stworzonej przez Wykonawcę na istniejącym serwerze w OPS przy wykorzystaniu serwerowego systemu operacyjnego dostarczanego przez Wykonawcę w ramach rozdziału 4.4 Zakup serwerowego systemu operacyjnego dla VM zarządzania bezpieczeństwem IT.

Wykonawca jest zobligowany wziąć pod uwagę zakres użytkowania oprogramowania dla OPS obejmujący następujące urządzenia:

1. komputery stacjonarne i laptopy - 35 szt.
2. drukarki w sieci – 16 szt.
3. serwer fizyczny pod wirtualizację – 1 szt.
4. serwer QNAP – 1 szt.
5. dysk sieciowy NAS – 1 szt.
6. UTM – 1 szt.
7. switchy – 2 szt.

Minimalne wymagania funkcjonalne dla oprogramowania do zarządzania bezpieczeństwem IT:

1. Oprogramowanie musi składać się serwera zarządzającego, zdalnych konsoli oraz Agentów.
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2.
3. Oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.
4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów - nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników.
5. Oprogramowanie musi posiadać funkcjonalność monitorowania infrastruktury serwerowej i sieciowej w zakresie:
  - a. wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
  - b. wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
  - c. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
  - d. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
  - e. serwerów pocztowych: - monitorowanie serwisu odbierającego, jak i wysyłającego pocztę, - możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), - możliwość wykonywania operacji testowych, - możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa,
  - f. monitorowania serwerów WWW i adresów URL,
  - g. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
  - h. obsługi komunikatów syslog i pułapek SNMP.

- i. monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych- ruchu generowanego przez podłączone stacje robocze,
  - j. kontroli nad monitorem usług Windows,
  - k. monitorowania wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
6. Oprogramowanie musi umożliwiać automatyczne gromadzenie danych o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie:
- a. informacji dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.;
  - b. zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;
  - c. informacji o zainstalowanych aplikacjach oraz aktualizacjach Windows, umożliwiających audytowanie i weryfikację użytkowania licencji w organizacji;
  - d. informacji o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.;
  - e. możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera;
  - f. możliwość odczytania numeru seryjnego (klucze licencyjne);
  - g. możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;
  - h. możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
7. Oprogramowanie musi mieć możliwość prowadzenia bazy ewidencji majątku IT w zakresie:
- a. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
  - b. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz, możliwość importu danych z zewnętrznego źródła np. (.CSV);
  - c. generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania;
  - d. archiwizacji i porównywania audytów środków trwałych;
  - e. tworzenia kodów kreskowych w Środkach Trwałych;
  - f. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy;
  - g. inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej co najmniej na system Android;
  - h. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji dodatkowego oprogramowania poprzez manualne wykonanie skanów inwentaryzacji offline).

8. Oprogramowanie musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
  - a. skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie, archiwów ZIP;
  - b. zarządzanie posiadanymi licencjami;
  - c. audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji;
  - d. zarządzanie posiadanymi licencjami: raport zgodności licencji;
  - e. możliwość przypisania do programów numerów seryjnych, wartości itp.
9. Oprogramowanie musi zapewniać integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
10. W zakresie pomocy technicznej system musi umożliwiać:
  - a. tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów);
  - b. załączanie komentarzy, zrzutów ekranów i załączników w zgłoszeniach;
  - c. konfigurowanie pól niestandardowych, powiązanych w wybraną kategorię zgłoszenia;
  - d. przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach”);
  - e. dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę;
  - f. planowanie zastępstw w przydzielaniu zgłoszeń;
  - g. funkcję rozbudowanych raportów;
  - h. powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym;
  - i. baza zgłoszeń z rozbudowaną wyszukiwarką;
  - j. przejrzysty i intuicyjny interfejs webowy;
  - k. wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych;
  - l. komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu;
  - m. zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury;
  - n. dwukierunkowa wymiana plików;
  - o. zarządzanie procesami Windows z poziomu okna informacji o urządzeniu;
  - p. zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania);
  - q. procesowanie zgłoszeń z wiadomości e-mail;
  - r. integracja bazy użytkowników z Active Directory;
  - s. zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).
11. W zakresie kontroli dostępu do danych system musi umożliwiać:
  - a. automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa;
  - b. ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych;
  - c. zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych;
  - d. integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania;

- e. integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych;
- f. możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB);
- g. alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”);
- h. integracja z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów
- i. zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami;
- j. informacje o urządzeniach podłączonych do danego komputera;
- k. lista wszystkich urządzeń podłączonych do komputerów w sieci;
- l. audyt (historia) połączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych;
- m. zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników;
- n. centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory.

#### 4.4. Zakup serwerowego systemu operacyjnego dla VM zarządzania bezpieczeństwem IT.

Aktualnie w Ośrodku Pomocy Społecznej w Sulechowie na serwerze użytkuje się oprogramowanie do wirtualizacji HyperV w oparciu o system Windows Serwer 2022 w wersji Standard. W ramach przedmiotowego zamówienia Wykonawca jest zobowiązany do dostarczenia dodatkowych licencji oprogramowania serwerowego systemu operacyjnego umożliwiającego mu uruchomienie jednego środowiska Windows Serwer 2022 w wersji Standard na jednej maszynie wirtualnej w środowisku HyperV przeznaczonej na potrzeby oprogramowania do zarządzania bezpieczeństwem IT (o którym mowa w rozdziale 4.3) na podstawie zasad licencjonowania producenta oprogramowania

lub dostawa równoważnej platformy systemowo-wirtualizacyjnej spełniającej minimalne kryteria równoważności określone poniżej.

Warunki równoważności dla dostawy równoważnej platformy systemowo-wirtualizacyjnej:

1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i siedmiu wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego dla minimum 20 użytkowników.
2. Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
3. 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.
4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.



6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
8. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
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 zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
15. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
16. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
17. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
18. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
19. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
20. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
21. W przypadku zaoferowania rozwiązania równoważnego Wykonawca jest zobligowany do instalacji, wdrożenia oraz migracji konfiguracji istniejącego środowiska OPS, w tym migracji wyrzyskich maszyn wirtualnych i danych do nowego rozwiązania równoważnego oraz przeprowadzenia szkolenia dla administratora w zakresie konfiguracji i eksploatacji na podstawie wcześniej zaakceptowanego przez Zamawiającego zakresu merytorycznego szkolenia.