



OPIS PRZEDMIOTU ZAMÓWIENIA

Przygotowany dokument ma na celu umożliwienie dokonania wyboru najkorzystniejszej oferty na dostawę i usługi teleinformatyczne, zgodne z rzeczywistymi potrzebami Jednostek Samorządu Terytorialnego (JST), których podstawowym celem jest zwiększenie poziomu cyberbezpieczeństwa i bezpieczeństwa informacji JST poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Dokument zawiera opis wymagań pod kątem kryteriów funkcjonalnych, technicznych oraz jakościowych, a także wskazuje technologie, które muszą być wykorzystane, aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania.

Wymagania ogólne dla urządzeń i oprogramowania

1. Dostarczony sprzęt musi być fabrycznie nowy (rok produkcji 2024), nieużywany, nieregenerowany, kompletny, dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”, rozwiązań odnawianych oraz eksponowanych na wystawach czy prezentacjach.
2. Sprzęt musi być wolny od wad fizycznych i prawnych, musi być sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanych rozwiązań, potwierdzające pochodzenie urządzeń z oficjalnego kanału dystrybucyjnego producenta.
3. Dostarczone oprogramowanie musi być nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania, nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) muszą być wolne od wad fizycznych i prawnych. Oprogramowanie musi być opatrzone we wszystkie atrybuty oryginalności i legalności wymagane przez producenta oprogramowania w zależności od dostarczanej wersji oprogramowania.



Cyberbezpieczny Samorząd

4. Serwis w ramach udzielonej gwarancji (podstawowej i/lub rozszerzonej) będzie realizowany bezpośrednio przez producenta i/lub we współpracy z autoryzowanym partnerem serwisowym producenta.
5. Wszystkie urządzenia powinny być zgodne z normami UE oraz powinny posiadać certyfikację oraz oznaczenie CE.
6. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy oferowanych zestawów oraz podzespoły montowane przez producenta były przez niego certyfikowane.
7. W formularzu ofertowym należy podać nazwę producenta, model, symbol (nazwę handlową) oraz parametry oferowanego rozwiązania (jeśli są wymagane) umożliwiające jednoznaczną weryfikację oferowanej konfiguracji oraz w celu identyfikacji należy podać pełną nazwę handlową oferowanego oprogramowania.

Ogólne warunki dla dokumentacji:

1. W przypadku wdrażanej konfiguracji poprawiającej cyberbezpieczeństwo Zamawiający wymaga dostarczenia dokumentacji opisującej wprowadzone zmiany.
2. W przypadku zmiany w infrastrukturze Zamawiający wymaga dostarczenia dokumentacji w ramach wprowadzonych zmian.

Warunki dotyczące realizacji dostaw i odbiorów:

1. Wykonawca na swój koszt i ryzyko dostarczy przedmiot zamówienia, zgodny z wymaganiami przedstawionymi w niniejszym dokumencie.
2. Wykonawca w cenie oferty uwzględni wszystkie koszty niezbędne do realizacji dostawy, w tym rozładunek, wniesienie oraz utrzymanie porządku w czasie rozładunku prowadzonego na terenie urzędu.
3. 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.
4. 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.
5. Do czasu odbioru sprzętu przez Zamawiającego, ryzyko wszelkich niebezpieczeństw związanych z jego ewentualnym uszkodzeniem lub utratą ponosi Wykonawca.
6. Wraz ze sprzętem Wykonawca zobowiązany jest przekazać Zamawiającemu listę numerów seryjnych dostarczonych urządzeń wszelką dokumentację dostarczoną przez producenta sprzętu.





Cyberbezpieczny Samorząd

7. W ramach procedury odbioru, Zamawiający zastrzega sobie w przypadku wątpliwości prawo do przeprowadzenia weryfikacji oryginalności i legalności dostarczonego przez Wykonawcę oprogramowania bezpośrednio u producenta oprogramowania, przed podpisaniem protokołu odbioru w sposób, który uzna za bezsporny. W przypadku wykrycia, że dostarczony system operacyjny lub inne licencjonowane oprogramowanie jest nieoryginalne (nielegalne), nie jest nowe, było już używane lub było już wcześniej aktywowane, Zamawiający w takiej sytuacji odmówi przyjęcia licencji oprogramowania i wezwie Wykonawcę do usunięcia nieprawidłowości w wyznaczonym terminie.

Warunki dotyczące realizacji usług:

Realizacja usług opisanych w niniejszym dokumencie 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.

Architektura projektowanego i uruchomionego rozwiązania informatycznego, o którym mowa w niniejszym dokumencie powinna spełnić wymagania określone w rozdziale IV rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, obowiązujących norm oraz standardów rynkowych. Zgodnie z zapisami §20 ust. 2 (KRI) system powinien spełniać wymagania w zakresie:

1. minimalizacji ryzyka utraty informacji w wyniku awarii,
2. zapewnienia bezpieczeństwa przechowywanych plików systemowych oraz innych,
3. zapewnienia możliwości regularnej aktualizacji oprogramowania (nowy system będzie posiadał wsparcie techniczne producenta w okresie eksploatacji).

Pozostałe wymagania:

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 jest zobowiązany uwzględnić w cenie w ramach kosztów dodatkowych:

1. Koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia (urządzeń) użytkownika 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 będą wymagane).



Cyberbezpieczny Samorząd

5. Koszty opracowania dokumentacji użytkowej (powykonawczej) oferowanego rozwiązania, aby administratorzy/użytkownicy mogli w sposób właściwy z niego korzystać.
6. Koszty uporządkowania oraz przywrócenia obiektu po wykonanych robotach do stanu pierwotnego wraz z naprawą ewentualnych szkód użytkownikowi lub osobom trzecim.

Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności min. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowanie 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 m. in. 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. Dbłość 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 spełniać wymagania przywołanych aktów prawnych oraz standardów rynkowych.

Zamawiający wymaga zaoferowania sprzętu informatycznego spełniającego wymagania podstawowe i (lub) opcjonalnie wymagania dodatkowe określone w niniejszym dokumencie oraz wykonania usług określonych w niniejszym dokumencie.

Szczegółowe wymagania w zakresie parametrów technicznych i funkcjonalnych poszczególnych elementów infrastruktury zostały określone w dalszej części dokumentu.



Cyberbezpieczny Samorząd

1. Opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Organizacyjny
Jednostka organizacyjna	Urząd Miejski Miejski Ośrodek Pomocy Społecznej Zespół Obsługi Placówek Oświatowych
Zakres	<p>Celem usługi jest zwiększenie ochrony danych i informacji w organizacji na poziomie technicznym oraz organizacyjnym, zapewnienie zgodności z obowiązującymi przepisami prawnymi, poprawa ogólnego poziomu bezpieczeństwa informacji zgodnie z normami wyrażonymi w PN ISO/IEC 27001. Zamawiający wymaga, aby usługa opracowania dokumentacji oraz wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) została zrealizowana zgodnie ze standardem ISO/IEC 27001:2022.</p> <p>Obszar ciągłości działania - dostępności informacji powinien być zgodny z wymaganiami normy ISO 22301:2019 - na zasadzie „best effort”.</p> <p>System powinien uwzględniać wdrożony system ochrony danych osobowych Zamawiającego.</p> <p>Wdrożenie powinno zostać przeprowadzone zgodnie z metodyką płynnego zarządzania - Agile.</p>

2. Audyt SZBI, audyt zgodności KRI/uoKSC

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Organizacyjny
Jednostka organizacyjna	Urząd Miejski Miejski Ośrodek Pomocy Społecznej Zespół Obsługi Placówek Oświatowych
Zakres	<p>Zadanie obejmuje przeprowadzenie audytu wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach organizacyjnych będących uczestnikami projektu.</p> <p>Audyt musi zostać przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu</p>





Cyberbezpieczny Samorząd

	<p>Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.</p> <p>Audyt musi zostać przeprowadzony w zakresie spełniającym wymagania określone w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem https://www.gov.pl/web/cppc/cyberbezpieczny-samorząd</p>
--	---

3. Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie usługą Active Directory w środowisku Windows Server

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Miejski
Zakres szkolenia	<p>Instalacja i konfiguracja kontrolerów domeny</p> <ol style="list-style-type: none">1. Omówienie usług AD DS2. Omówienie kontrolerów domeny usług AD DS3. Wdrożenie kontrolera domeny4. Encrypted DNS - szyfrowana usługa rozpoznawania nazw w Windows Server 2022 <p>Zarządzanie obiektami w AD DS</p> <ol style="list-style-type: none">1. Zarządzanie kontami użytkowników2. Zarządzanie grupami w usługach AD DS3. Zarządzanie obiektami typu komputer w AD DS4. Wdrażanie i zarządzanie OU <p>Zarządzanie zaawansowaną infrastrukturą AD DS</p> <ol style="list-style-type: none">1. Wprowadzenie do zaawansowanych wdrożeń AD DS2. Wdrożenie rozproszonego środowiska AD DS3. Konfiguracja relacji zaufania AD DS <p>Wdrażanie i zarządzanie lokacjami i repliką AD DS</p> <ol style="list-style-type: none">1. Omówienie replikacji usług AD DS2. Konfigurowanie lokacji usług AD DS3. Konfigurowanie i monitorowanie replikacji usług AD DS





Cyberbezpieczny Samorząd

	<p>Wdrażanie zasad grupy</p> <ol style="list-style-type: none">1. Wprowadzenie do zasad grupy2. Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)3. Konfiguracja zakresu i przetwarzania obiektów GPO4. Rozwiązywanie problemów z GPO <p>Zarządzanie ustawieniami użytkowników za pomocą zasad grupy</p> <ol style="list-style-type: none">1. Wdrażanie szablonów administracyjnych2. Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów3. Konfiguracja preferencji zasad grupowych
Typ szkolenia	Szkolenie stacjonarne (wyjazdowe)
Liczba uczestników	2 osoby
Czas trwania	Minimum 2 dni dla każdej osoby
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie.
Obowiązki Wykonawcy	<p>Obowiązkiem Wykonawcy będzie zapewnienie:</p> <ol style="list-style-type: none">1. Szkoleń (warsztatów) w formie stacjonarnej prowadzonych przez wieloletniego praktyka i szkoleniowca.2. Pakietu materiałów szkoleniowych.3. W trakcie szkoleń: lunch + przerwy kawowe.4. Preferowane szkolenia w południowej części Polski.
Obowiązki Zamawiającego	<p>Obowiązkiem Zamawiającego będzie zapewnienie:</p> <ol style="list-style-type: none">1. Transportu uczestnika do miejsca odbycia szkolenia.2. Noclegu dla uczestnika szkolenia.

4. Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i administrowanie systemami Windows Server

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Miejski
Zakres szkolenia	<p><u>Wprowadzenie do administracji systemu Windows Server</u></p> <ol style="list-style-type: none">1. Wprowadzenie do systemu Windows Server2. Wprowadzenie do systemu Windows Server Core





Cyberbezpieczny Samorząd

3. Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server.

Usługi zarządzania tożsamością w systemie Windows Server

1. Wprowadzenie do AD DS
2. Wdrażanie kontrolerów domeny Windows Server
3. Wprowadzenie do usługi Azure AD
4. Wdrażanie zasad grupy
5. Wprowadzenie do usług certyfikatów Active Directory

Usługi infrastruktury sieciowej w systemie Windows Server

1. Wdrażanie i zarządzanie protokołem DHCP
2. Wdrażanie i zarządzanie systemem DNS
3. Wdrażanie i zarządzanie systemem IPAM
4. Usługi dostępu zdalnego w systemie Windows Server

Serwery plików i zarządzanie pamięcią masową w systemie Windows Server

1. Woluminy i systemy plików w systemie Windows Server
2. Wdrażanie udostępniania w systemie Windows Server
3. Wdrażanie rozwiązania Storage Spaces (przestrzeni dyskowych) w systemie Windows Server
4. Wdrażanie deduplikacji danych
5. Wdrażanie interfejsu iSCSI
6. Wdrażanie rozproszonego systemu plików

Wirtualizacja Hyper-V i kontenery w systemie Windows Server

1. Hyper-V w systemie Windows Server
2. Konfiguracja maszyn wirtualnych
3. Zabezpieczanie wirtualizacji w systemie Windows Server
4. Kontenery w systemie Windows Server
5. Wprowadzenie do platformy Kubernetes w systemie Windows

Wysoka dostępność w systemie Windows Server

1. Planowanie wdrożenia klastra pracy awaryjnej
 2. Tworzenie i konfiguracja klastra pracy awaryjnej
 3. Wprowadzenie do rozciągniętych klastrów
- Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V





Cyberbezpieczny Samorząd

	<p><u>Odzyskiwanie danych po awarii w systemie Windows Server</u></p> <ol style="list-style-type: none">1. Funkcja Hyper-V Replica2. Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server <p><u>Bezpieczeństwo systemu Windows Server</u></p> <ol style="list-style-type: none">1. Ochrona danych uwierzytelniających i dostępu uprzywilejowanego2. Hardening systemu Windows Server3. JEA w systemie Windows Server4. Zabezpieczanie i analiza ruchu w SMB5. Zarządzanie aktualizacjami w systemie Windows Server <p><u>RDS (usługi pulpitu zdalnego) w systemie Windows Server</u></p> <ol style="list-style-type: none">1. Wprowadzenie do RDS2. Konfiguracja wdrażania pulpitu opartego na sesji3. Wprowadzenie do osobistych i połączonych pulpitów wirtualnych <p><u>Dostęp zdalny i usługi internetowe w systemie Windows Server</u></p> <ol style="list-style-type: none">1. Wdrażanie sieci VPN2. Wdrażanie usługi Always On VPN3. Wdrażanie systemu NPS4. Wdrażanie serwera WWW w systemie Windows Server <p><u>Monitorowanie serwera i wydajności w systemie Windows Server</u></p> <ol style="list-style-type: none">1. Wprowadzenie do narzędzi do monitorowania systemu Windows Server2. Korzystanie z monitora wydajności3. Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów <p><u>Aktualizacja i migracja w systemie Windows Server</u></p> <ol style="list-style-type: none">1. Migracja AD DS2. Usługa migracji pamięci masowej3. Narzędzia do migracji systemu Windows Server
Typ szkolenia	Szkolenie stacjonarne (wyjazdowe)
Liczba uczestników	2 osoby
Czas trwania	Minimum 5 dni dla każdej osoby



Cyberbezpieczny Samorząd

Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie. <u>Zamawiający wymaga zapewnienia szkolenia prowadzonego przez autoryzowanego trenera Microsoft (MCT).</u>
Obowiązki Wykonawcy	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. Preferowane szkolenia w południowej części Polski.
Obowiązki Zamawiającego	Obowiązkiem Zamawiającego będzie zapewnienie: 1. Transportu uczestnika do miejsca odbycia szkolenia. 2. Noclegu dla uczestnika szkolenia.

5. Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i administrowanie rozwiązaniem UTM na poziomie „Administrator”

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Miejski
Zakres szkolenia	<p>Zamawiający oczekuje zapewnienia uczestnictwa w szkoleniu dedykowanym specjalistom ds. sieci i bezpieczeństwa zajmującym się zarządzaniem, konfiguracją, administracją i monitorowaniem urządzeń FortiGate używanych do zabezpieczania sieci. Szkolenie ma na celu poznać najpopularniejsze funkcje rozwiązań FortiGate za pomocą uczestnictwa w wykładach oraz uczestnictwa w interaktywnych laboratoriach, gdzie zostaną przedstawione zasady m.in. zapory ogniowej, uwierzytelnianie użytkowników, wysokiej dostępności, SSL VPN, VPN typu site-to-site IPsec, Fortinet Security Fabric oraz sposoby ochrony sieci za pomocą profili zabezpieczeń, takich jak IPS, program antywirusowy, filtrowanie sieci, kontrola aplikacji i inne.</p> <p>Ramowy zakres szkolenia:</p> <ol style="list-style-type: none">1. Ustawienia systemowe i sieciowe, konfiguracja sieci.2. Zasady zapory sieciowej i NAT.



Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">3. Routing, analiza tras.4. Uwierzytelnianie.5. Monitorowanie użytkowników.6. Dostęp Fortinet Single Sign-On (FSSO) do usług sieciowych, zintegrowany z Microsoft Active Directory (AD).7. Antivirus.8. Web Filtering.9. Zapobieganie włamaniom i kontrola aplikacji.10. SSL VPN.11. IPsec VPN.12. Konfiguracja i monitorowanie SD-WAN.13. Budowa klastra High Availability w celu zapewnienia odporności na awarie oraz zapewnienia wysokiej wydajności.14. Diagnostyka i rozwiązywanie problemów.
Typ szkolenia	On-line
Liczba uczestników	2 osoby
Czas trwania	Minimum 4 dni dla każdej osoby
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie. <u>Zamawiający wymaga zapewnienia szkolenia prowadzonego przez autoryzowanego trenera Fortinet Certified Trainer (FCT).</u>

6. Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i administrowanie rozwiązaniem UTM na poziomie „Immersion”

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Miejski
Zakres szkolenia	Zamawiający oczekuje zapewnienia uczestnictwa w szkoleniu opartym na zadaniach konfiguracyjnych w środowisku wirtualnego laboratorium. Zadania powinny obejmować najpopularniejszych funkcji FortiGate, takie jak zasady zapory ogniowej, Fortinet Security Fabric, uwierzytelnianie użytkowników, sieci VPN SSL i IPsec, routing, IPS, wysoka dostępność (HA) i inne.
Typ szkolenia	On-line





Cyberbezpieczny Samorząd

Liczba uczestników	2 osoby
Czas trwania	Minimum 1 dzień dla każdej osoby
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie. <u>Zamawiający wymaga zapewnienia szkolenia prowadzonego przez autoryzowanego trenera Fortinet Certified Trainer (FCT).</u>

7. Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i administrowanie rozwiązaniem dla posiadanego oprogramowania do zarządzania zasobami IT

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Miejski
Zakres szkolenia	<p>Plan szkolenia z obsługi i konfiguracji oprogramowania specjalistycznego do zarządzania zasobami IT „Axence nVision” będącego w posiadaniu Zamawiającego powinien obejmować:</p> <ol style="list-style-type: none">1. Ogólne omówienie programu.2. Konfiguracja systemu i instalacja.3. Konfiguracja i praca we wszystkich modułach.4. Rozwiązywanie najczęstszych problemów. <p>Podczas szkolenia (warsztatów) administrator ma:</p> <ol style="list-style-type: none">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 niejednorodną konfiguracją programową i sprzętową swoich stacji, wykonania audytu oprogramowania,



Cyberbezpieczny Samorząd

	<p>plików multimedialnych, zwiększenia swoich umiejętności w obszarze zarządzania środkami trwałymi.</p> <p>6. Zdobyć umiejętności w obszarze monitorowania aktywności użytkowników, tak aby można było szybko i jednoznacznie analizować ich pracę i jednocześnie dbać o bezpieczeństwo organizacji.</p> <p>7. Zdobyć umiejętności pozwalające na rozliczalność komunikacji „użytkownik-IT”, na zbudowanie bazy wiedzy dla pracowników, na zautomatyzowanie procesów związanych z obsługą zgłoszeń serwisowych.</p> <p>8. Zdobyć umiejętności w zakresie zarządzania nośnikami zewnętrznymi, rozliczania pracy z nimi oraz rozliczania pracy na plikach wspólnych.</p> <p>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.</p> <p>10. Zdobyć umiejętność skonfigurowania widżetów prezentujących kluczowe parametry, historię pracy sieci oraz informacje o działaniach użytkowników.</p>
Typ szkolenia	Szkolenie stacjonarne (wyjazdowe)
Liczba uczestników	2 osoby
Czas trwania	Minimum 14 godzin lekcyjnych (2d x 7h) przy założeniu, że jedna godzina lekcyjna trwa 45 min
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie.
Obowiązki Wykonawcy	<p>Obowiązkiem Wykonawcy będzie zapewnienie:</p> <ol style="list-style-type: none">1. Szkoleń (warsztatów) w formie stacjonarnej prowadzonych przez wieloletniego praktyka i szkoleniowca.2. Pakietu materiałów szkoleniowych.3. W trakcie szkoleń: lunch + przerwy kawowe.4. Preferowane szkolenia w południowej części Polski.
Obowiązki Zamawiającego	<p>Obowiązkiem Zamawiającego będzie zapewnienie:</p> <ol style="list-style-type: none">1. Transportu uczestnika do miejsca odbycia szkolenia.2. Noclegu dla uczestnika szkolenia.





Cyberbezpieczny Samorząd

8. Zakup szkoleń dla kadry pracowniczej z cyberbezpieczeństwa

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Miejski Miejski Ośrodek Pomocy Społecznej Zespół Obsługi Placówek Oświatowych
Zakres szkoleń	<p>Zamawiający wymaga zorganizowania przez Wykonawcę szkoleń mających na celu podniesienie świadomości pracowników urzędu z zakresu cyberbezpieczeństwa oraz budowania umiejętności radzenia sobie z cyberzagrożeniami. 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.</p> <p>Wymagana jest realizacja cyklu szkoleń w formie wykładu.</p> <ol style="list-style-type: none">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. <p>Zakres szkolenia:</p> <ol style="list-style-type: none">1. Główne założenia i wymagania prawne RODO, KRI, KSC.2. Incydent bezpieczeństwa komputerowego i RODO - zasady postępowania w przypadku jego wystąpienia.3. Naruszenie ochrony danych osobowych i zasady postępowania w przypadku jego wystąpienia.4. Podstawowe zasady bezpieczeństwa (bezpieczeństwo fizyczne):<ol style="list-style-type: none">a) Zasada czystego biurka;b) Zasada czystego ekranu;c) Zasada czystego wydruku;d) Zasada czystego kosza;5. Polityka bezpiecznych haseł (menadżer haseł, generowanie i dobór haseł, postępowanie z hasłami).6. Najczęściej wykorzystywane metody ataków (socjotechnika, phishing,



Cyberbezpieczny Samorząd

	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.
Typ szkolenia	Szkolenie stacjonarne w podziale na grupy (w siedzibie urzędu)
Liczba uczestników	Łącznie 70 osób w podziale na: Urząd Miejski - 45 osób Miejski Ośrodek Pomocy Społecznej - 16 osób Zespół Obsługi Placówek Oświatowych - 9 osób
Czas trwania	Minimum 2 godziny lekcyjne dla każdej grupy przy założeniu, że jedna godzina lekcyjna trwa 45 min.
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie.
Obowiązki Wykonawcy	Obowiązkiem Wykonawcy będzie zapewnienie: 1. Kadry trenerskiej posiadającej wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolnej do pełnej realizacji wymogów związanych z prowadzeniem szkoleń. 2. Pakietu materiałów szkoleniowych. 3. Wydanie uczestnikom szkolenia zaświadczeń o ukończeniu szkolenia. 4. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się: a) lista obecności uczestników szkolenia (prowadzona oddzielnie dla każdej grupy, b) lista potwierdzająca odbiór zaświadczeń o ukończeniu szkolenia. 5. Sprzętu elektronicznego (laptop, projektor) niezbędnego do prowadzenia szkolenia.
Obowiązki Zamawiającego	Obowiązkiem Zamawiającego będzie zapewnienie: 1. Nieodpłatne udostępnienie lokalu (szali szkoleniowej dla wymaganej liczby uczestników) z dostępem do Internetu oraz energii elektrycznej. 2. Rekrutacji osób biorących udział w szkoleniach oraz ustalenie składu grup - w przypadku nieobecności uczestnika na zajęciach prowadzonych w ramach jego grupy szkoleniowej, uczestnik może dołączyć do innej grupy.

9. Zakup serwerów (typ 1) do pracy w klastrze wysokiej dostępności HA (High Availability Cluster)



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	Łącznie 2 zestawy dla jednostki organizacyjnej: Urząd Miejski
Funkcjonalność obudowy	<ul style="list-style-type: none">Obudowa Rack o wysokości max 1U, wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych.Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Funkcjonalność płyty głównej	<p>Płyta główna wyposażona w:</p> <ul style="list-style-type: none">16 slotów pamięci RAM przeznaczonych do instalacji pamięci RAM,Min. 3 sloty PCIeMin. 2 gniazda (sockety) pod procesory, zapewniająca obsługę procesorów 32 rdzeniowych
Procesor	<p>Zainstalowane dwa procesory wielordzeniowe dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 175 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.</p> <p><i>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.</i></p>
Pamięć RAM	<p>256 GB pamięci RAM z możliwością rozbudowy do 1TB RAM.</p> <p>Wymagane funkcjonalności pamięci RAM: Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection.</p>
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none">2 interfejsy 1GbE w standardzie Base-T4 interfejsy 25GbE w standardzie SFP28





Cyberbezpieczny Samorząd

Dyski twarde	Min. 2 dyski M.2 NVMe SSDs o pojemności min. 480GB każdy (Hot-Plug) z możliwością konfiguracji RAID 1.
Porty/złącza	<ul style="list-style-type: none">4x USB, w tym co najmniej 1x USB 3.02x VGA
Karta graficzna	Karta graficzna umożliwiająca pracę w rozdzielczości 1920x1200
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz Hot-Plug o mocy min. 1100W klasy Titanium (1+1)
Bezpieczeństwo	<ul style="list-style-type: none">Zatrzaśka górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.Możliwość wyłączenia w BIOS funkcji przycisku zasilania.BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.Moduł TPM 2.0Wymagana możliwość dynamicznego włączania i wyłączania portów USB na obudowie - bez potrzeby restartu serwera.Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera - niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta zarządzająca	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: <ul style="list-style-type: none">zdalny dostęp do graficznego interfejsu Web karty zarządzającej;zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;możliwość podmontowania zdalnych wirtualnych napędów;wirtualną konsolę z dostępem do myszy, klawiatury;





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ wsparcie dla IPv6;▪ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;▪ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;▪ integracja z Active Directory;▪ możliwość obsługi przez dwóch administratorów jednocześnie;▪ wsparcie dla dynamic DNS;▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;▪ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;▪ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: wirtualny schowek ułatwiający korzystanie z konsoli zdalnej, przesyłanie danych telemetrycznych w czasie rzeczywistym, dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze, automatyczną rejestrację certyfikatów (ACE).
Oprogramowanie do zarządzania	<p>Wymagana możliwość zainstalowania oprogramowania do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none">▪ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych.▪ Integracja z Active Directory.▪ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta.▪ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish.▪ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram.▪ Szczegółowy opis wykrytych systemów oraz ich komponentów.▪ Możliwość eksportu raportu do CSV, HTML, XLS, PDF.▪ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.▪ Grupowanie urządzeń w oparciu o kryteria użytkownika.



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji.▪ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach.▪ Szybki podgląd stanu środowiska.▪ Podsumowanie stanu dla każdego urządzenia.▪ Szczegółowy status urządzenia/elementu/komponentu.▪ Generowanie alertów przy zmianie stanu urządzenia.▪ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń.▪ Integracja z service desk producenta dostarczonej platformy sprzętowej.▪ Możliwość przejęcia zdalnego pulpitu.▪ Możliwość podmontowania wirtualnego napędu.▪ Kreator umożliwiający dostosowanie akcji dla wybranych alertów.▪ Możliwość importu plików MIB.▪ Przesyłanie alertów „as-is” do innych konsol firm trzecich.▪ Możliwość definiowania ról administratorów.▪ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów.▪ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania).▪ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta.▪ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów.▪ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.▪ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.▪ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile.
--	--





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.Zdalne uruchamianie diagnostyki serwera.Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Gwarancja i serwis	Min. 2 lata (24 miesiące)
Warunki gwarancji	<ul style="list-style-type: none">Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych)Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej/ internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.Zamawiający wymaga gwarancji uwzględniającej zabezpieczenie serwisowe, które w przypadku awarii dysku twardego (w urządzeniu objętym aktywnym





Cyberbezpieczny Samorząd

	<p>wparciem technicznym) powodującej konieczność jego wymiany, umożliwi pozostawienie uszkodzonego dysku u Zamawiającego (dysk nie będzie podlegał ekspertyzie poza siedzibą Zamawiającego).</p> <ul style="list-style-type: none">▪ Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocenę bezpieczeństwa cybernetycznego.▪ Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń.
Certyfikaty, normy i standardy	<ul style="list-style-type: none">▪ Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie produkcji - <i>dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</i>▪ Spełnianie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie produkcji - <i>dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</i>▪ Spełnianie normy ISO 50001 lub równoważnej dla producenta sprzętu w zakresie produkcji - <i>dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</i>▪ Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.▪ Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.▪ Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-





Cyberbezpieczny Samorząd

	gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. <i>Dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku.</i>
Komponenty	2 x kabel direct attach 10GbE SFP+ o długości min. 3 metry.

Atrybut	Wymagania <u>dodatkowe</u> (fakultatywne, nieobowiązkowe)
Uszczegółowienie	Za spełnienie wymagania dodatkowego Wykonawcy zostanie przyznana liczba punktów określona w pozostałych kryteriach oceny ofert zgodnie z kryteriami określonymi w rozdziale 16 SWZ.
Dodatkowy okres gwarancji (wymaganie nieobowiązkowe)	<p>Zaoferowanie serwerów z dodatkową gwarancją udzieloną przez producenta lub gwarancją udzieloną przez autoryzowany serwis producenta serwerów 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 serwerów do pracy w klastrze wysokiej dostępności - typ 1 (S1).</p> <p>W przypadku zaoferowania gwarancji wydłużającej gwarancję podstawową, okres zabezpieczenia serwisowego na nośniki pamięci masowej (dyski twarde), musi być tożsamy z czasem gwarancji udzielonej na serwery po wydłużeniu gwarancji podstawowej.</p> <p><u>Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.</u></p>

10. Zakup licencji na serwerowy system operacyjny

Atrybut	Wymagania <u>minimalne, podstawowe, obligatoryjne, obowiązkowe</u>
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego oprogramowania
Ilość	Wymagane jest dostarczenie licencji dla 2 serwerów typ 1 dla jednostki organizacyjnej: Urząd Miejski





Cyberbezpieczny Samorząd

Oprogramowanie musi zostać dostarczone dla serwera fizycznego wyposażonego w 2 procesory wielordzeniowe. Jeśli dobór licencji zależy od liczby rdzeni procesora, Zamawiający ma obowiązek dostarczyć właściwą liczbę licencji dla liczby rdzeni procesora w oferowanym serwerze. Zamawiający wymaga dostarczenia licencji na oprogramowanie (system serwerowy) w najnowszej wersji obecnie dostępnej na rynku.

Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczby (bez ograniczeń) wirtualnych środowisk serwerowego systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

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:
 - a) pozwalają na zmianę rozmiaru w czasie pracy systemu,





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). <p>10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</p> <p>11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</p> <p>12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET</p> <p>13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</p> <p>14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</p> <p>15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:</p> <ul style="list-style-type: none">a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,b) dotykowy umożliwiający sterowanie dotykaniem na monitorach dotykowych. <p>16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</p> <p>17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.</p> <p>18. Mechanizmy logowania w oparciu o:</p> <ul style="list-style-type: none">a) Login i hasło,b) Karty z certyfikatami (smartcard),c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), <p>19. 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..</p> <p>20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).</p>
--	--





Cyberbezpieczny Samorząd

	<p>21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</p> <p>23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).</p> <p>24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none">a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:<ul style="list-style-type: none">▪ Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,▪ Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,▪ Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.▪ Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.c) Zdalna dystrybucja oprogramowania na stacje robocze.d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczeje) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:<ul style="list-style-type: none">▪ Dystrybucję certyfikatów poprzez http▪ Konsolidację CA dla wielu lasów domeny,
--	---





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,▪ Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. <p>f) Szyfrowanie plików i folderów.</p> <p>g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</p> <p>h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.</p> <p>i) Serwis udostępniania stron WWW.</p> <p>j) Wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>k) Wsparcie dla algorytmów Suite B (RFC 4869),</p> <p>l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,</p> <p>m) 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:</p> <ul style="list-style-type: none">▪ 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)
--	---





Cyberbezpieczny Samorząd

	<p>26. 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.</p> <p>27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p> <p>28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p>
--	---

11. Zakup macierzy pamięci masowej

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	1 komplet Jednostka organizacyjna: Urząd Miejski
Obudowa	Do instalacji w standardowej szafie Rack 19", macierz musi zajmować maksymalnie 2U i pozwalać na instalacje min. 24 dysków 2.5".
Pamięć masowa	<ul style="list-style-type: none">▪ Zainstalowane 24 dyski SAS Hot-Plug o pojemności min. 2.4TB każdy.▪ Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".▪ Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
Sposób zabezpieczenia danych	<ul style="list-style-type: none">▪ Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.▪ Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).▪ Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć Cache	<ul style="list-style-type: none">▪ Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.▪ Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.▪ Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.▪ Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.▪ Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać co najmniej 8 portów 25Gb iSCSI (4 porty na kontroler)
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	<ul style="list-style-type: none">▪ Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.▪ Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.▪ Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.



Cyberbezpieczny Samorząd

Thin Provisioning	<ul style="list-style-type: none">Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	<ul style="list-style-type: none">Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	<ul style="list-style-type: none">Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na



Cyberbezpieczny Samorząd

	podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „Hot-Swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania - odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych



Cyberbezpieczny Samorząd

	<p>przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.</p> <p>Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.</p>
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Gwarancja i serwis	Min. 2 lata (24 miesiące)
Warunki gwarancji	<ul style="list-style-type: none">▪ Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.▪ Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych)▪ Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.▪ Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.▪ Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.▪ Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej/ internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.▪ Zamawiający wymaga gwarancji uwzględniającej zabezpieczenie serwisowe, które w przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wsparciem technicznym) powodującej konieczność jego wymiany, umożliwi pozostawienie uszkodzonego dysku u Zamawiającego (dysk nie będzie podlegał ekspertyzie poza siedzibą Zamawiającego).





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocenę bezpieczeństwa cybernetycznego.▪ Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń.
Certyfikaty	<ul style="list-style-type: none">▪ Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie produkcji - <i>dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</i>▪ Spełnianie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie produkcji - <i>dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</i>▪ Spełnianie normy ISO 50001 lub równoważnej dla producenta sprzętu w zakresie produkcji - <i>dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</i>
Komponenty	4 x kabel direct attach 25GbE SFP28 o długości min. 3 metry.

Atrybut	Wymagania <u>dodatkowe</u> (fakultatywne, nieobowiązkowe)
Uszczegółowienie	Za spełnienie wymagania dodatkowego Wykonawcy zostanie przyznana liczba punktów określona w pozostałych kryteriach oceny ofert zgodnie z kryteriami określonymi w rozdziale 16 SWZ.
Dodatkowy okres gwarancji (wymaganie nieobowiązkowe)	<p>Zaoferowanie macierzy pamięci masowej z dodatkową gwarancją udzieloną przez producenta lub gwarancją udzieloną przez autoryzowany serwis producenta macierzy 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 macierzy pamięci masowej (M).</p> <p>W przypadku zaoferowania gwarancji wydłużającej gwarancję podstawową, okres zabezpieczenia serwisowego na nośniki pamięci masowej (dyski twarde), musi być</p>



Cyberbezpieczny Samorząd

	tożsamy z czasem gwarancji udzielonej na macierz po wydłużeniu gwarancji podstawowej. <u>Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.</u>
--	--

12. Zakup dysków do posiadanej macierzy produkcyjnej

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	Łącznie 17 sztuk dla jednostki organizacyjnej: Urząd Miejski
Zastosowanie	Dysk twardy do macierzy Dell EMC ME5024
Parametry	W celu zachowania pełnej kompatybilności z posiadanymi dyskami w macierzy Zamawiający wymaga dostarczenia dysków 2,5 cala o pojemności min. 2.4TB, interfejs SAS 12Gb/s, prędkość obrotowa 10000 obr/min, w pakiecie obudowa dysku do instalacji Hot-Plug.

13. Zakup serwera NAS (typ 1) z dyskami

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	1 komplet Jednostka organizacyjna: Urząd Miejski
Funkcjonalność obudowy	<ul style="list-style-type: none">Do instalacji w standardowej szafie typu Rack 19", serwer musi zajmować maksymalnie wysokość 2U, w zestawie szyny do montażu serwera w szafie typu Rack.Możliwość instalacji 12 dysków.Wyposażona w gniazda USB: 2x USB 3.2 Gen 2 (10 Gb/s)Wyposażona we wskaźniki LED informujące o statusach: HDD 1-12, stan, LAN



Cyberbezpieczny Samorząd

Procesor	Wymagany procesor wielordzeniowy, umożliwiający osiągnięcie w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik min. 33.000 punktów. <i>Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony www.cpubenchmark.net</i>
Pamięć operacyjna	min. 64 GB z możliwością rozbudowy do 192GB
Pamięć masowa	<ul style="list-style-type: none">▪ Dyski twarde 8 sztuk o pojemności 10TB każdy.▪ Dyski twarde klasy Enterprise przystosowane do zapisu ciągłego, zgodne z listą kompatybilności producenta oferowanego sprzętu.
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
System plików	<ul style="list-style-type: none">▪ Dyski wewnętrzne ZFS lub EXT4.▪ Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Funkcje ZFS	Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
RAID	<ul style="list-style-type: none">▪ Obsługiwane typy macierzy RAID: 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy.▪ Funkcje RAID: Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Interfejsy sieciowe	2x 2,5 GbE RJ-45 2x 10 GbE RJ-45 2x 10 GbE SFP+
Język GUI	Polski
Zasilanie	<ul style="list-style-type: none">▪ Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz (1+1)▪ Wymagana obsługa sieciowych awaryjnych zasilaczy UPS.
Funkcja udostępniania plików	<ul style="list-style-type: none">▪ Liczba kont użytkowników: 16000▪ Liczba grup użytkowników: 500▪ Liczba udziałów: 100▪ Liczba jednoczesnych połączeń (CIFS): 5000▪ Liczba migawek: 65000



Cyberbezpieczny Samorząd

Wsparcie dla systemów	<ul style="list-style-type: none">▪ Apple Mac OS 10.10 or later▪ Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub starszy Linux▪ IBM AIX 7, Solaris 10 or later UNIX▪ Microsoft Windows 7, 8, 10, and 11▪ Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022
Gwarancja i serwis	Min. 2 lata (24 miesiące)
Warunki gwarancji	<ul style="list-style-type: none">▪ Pomoc telefoniczna lub e-mailowa przy uruchomieniu i wdrożeniu produktu.▪ Wsparcie techniczne w przypadku problemów ze współpracą z innymi elementami sieci.▪ Pełna asysta telefoniczna (lub e-mailowa) przy aktualizacji oprogramowania.▪ Pomoc techniczna w sprawach nietypowych, modyfikacjach oprogramowania itp.▪ Priorytetowy tryb rozpatrywania gwarancji i prowadzenia naprawy.▪ Realizacja naprawy w siedzibie w miejscu instalacji sprzętu, lub zapewnienie sprzęt zastępczego na czas naprawy (wymagana dostawa zastępczego urządzenia w przeciągu 24h od zgłoszenia).▪ Pomoc przy migracji danych na nowy serwer.

Atrybut	Wymagania <u>dodatkowe</u> (fakultatywne, nieobowiązkowe)
Uszczegółowienie	Za spełnienie wymagania dodatkowego Wykonawcy zostanie przyznana liczba punktów określona w pozostałych kryteriach oceny ofert zgodnie z kryteriami określonymi w rozdziale 16 SWZ.
Dodatkowy okres gwarancji (wymaganie nieobowiązkowe)	<p>Zaoferowanie serwera NAS (typ 1) z dodatkową gwarancją udzieloną przez producenta lub gwarancją udzieloną przez autoryzowany serwis producenta serwera 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 macierzy pamięci masowej (S3).</p> <p><u>Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.</u></p>



Cyberbezpieczny Samorząd

14. Zakup zasilaczy awaryjnych UPS do serwerów

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	Łącznie 4 zestawy dla jednostek organizacyjnych: <ul style="list-style-type: none">▪ Urząd Miejski - 2 zestawy▪ Miejski Ośrodek Pomocy Społecznej - 1 zestaw▪ Zespół Obsługi Placówek Oświatowych - 1 zestaw
Obudowa	Typu Rack, wysokość 2U, w zestawie szyny montażowe do szafy Rack 19''
Technologia	VFI-SS-111 zgodnie z PN-EN62040-3 (true on-line, podwójne przetwarzanie energii)
Moc znamionowa	3 kVA / 3 kW
Wyjściowy współczynnik mocy (PF)	1,0
Napięcie wejściowe	230 Vac
Sposób zasilania	Plug&Play Gniazdo w standardzie IEC 320
Tolerancja napięcia wejściowego	161 – 299 V przy obciążeniu 50-100%; bez przechodzenia na baterie 115 – 299 Vac przy obciążeniu mniejszym od 50%; bez przechodzenia na baterie
Częstotliwość wejściowa	Wymagana 50 Hz +/-20%
Sprawność AC-AC	<ul style="list-style-type: none">▪ nie mniejsza niż 93% w trybie pracy on-line z obciążeniem 100%▪ nie mniejsza niż 99% w trybie pracy Oszczędzania energii Eco Mode
Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.
Napięcie wyjściowe	230 V
Częstotliwość wyjściowa	50/60Hz (programowalna)
Zintegrowane bezprzerwowe	Statyczny przełącznik (SCR) z możliwością ręcznego przełączenia UPSa do trybu Bypass elektroniczny



Cyberbezpieczny Samorząd

przełączniki obejściowy Bypass	
Czas podtrzymania (wg karty katalogowej producenta)	<ul style="list-style-type: none">▪ nie mniej niż 4 minuty przy 100% obciążenia▪ nie mniej niż 11 minut przy 50% obciążenia
Złącze baterii zewnętrznych	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): <ul style="list-style-type: none">▪ przy 50% obciążeniu nie mniej niż 47 minut▪ przy 100% obciążeniu nie mniej niż 20 minut
Akumulatory	<ul style="list-style-type: none">▪ Szczelne, bezobsługowe, technologia AGM, o projektowanej żywotności min. 10 lat,▪ Baterie w UPS do wymiany w trybie HotSwap oraz możliwość odłączenia modułu bateryjnego za pomocą wtyczki
Układ ładowania akumulatorów o konfigurowalnych parametrach	Możliwość ładowania akumulatorów prądem w zakresie 1 – 8A konfigurowalnym z LCD (bez konieczności stosowania oprogramowania serwisowego)
Stabilizacja napięcia wyjściowego	<ul style="list-style-type: none">▪ w stanie ustalonym $\pm 1\%$▪ w stanie nieustalonym $\pm 3\%$
Stabilność częstotliwości wyjściowej:	bez synchronizacji: $\pm 0,1\%$
Współczynnik szczytu	3:1
Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD oraz sygnalizacją akustyczną	Wymagane ze wskazaniem parametrów napięcia wejściowego i wyjściowego, częstotliwości, pozostałego czasu pracy podczas pracy bateryjnej.
Interfejsy	Złącze interfejsów komunikacyjnych: RS232, USB, slot SNMP



Cyberbezpieczny Samorząd

	Interfejs EPO (do wyłącznika ppoż.)
Gniazda wyjściowe IEC320 na zasilaczu UPS	Wymagane minimum gniazd: 8x 10A oraz 1x 16A
Oprogramowanie	Wymagane oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego.
Poziom hałasu w odległości 1m,	< 48 dBA Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury
Możliwość regulacji z oprogramowania tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Regulacja z Panela LCD
Wyposażenie dodatkowe	Wraz z zasilaczem musi zostać dostarczona karta SNMP do zarządzania UPS z poziomu sieci.
Normy, certyfikaty i standardy	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa, kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE
Gwarancja i serwis	Min. 2 lata (24 miesiące)

15. Zakup zasilaczy awaryjnych UPS do stanowisk komputerowych

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	Łącznie 70 sztuk dla jednostek organizacyjnych: <ul style="list-style-type: none">▪ Urząd Miejski - 45 sztuk▪ Miejski Ośrodek Pomocy Społecznej - 16 sztuk▪ Zespół Obsługi Placówek Oświatowych - 9 sztuk
Moc pozorna	min. 800VA
Obudowa	Tower wyposażona w graficzny wyświetlacz LCD
Klasa	Line-interactive



Cyberbezpieczny Samorząd

Kształt napięcia	Sinusoida
Funkcjonalności	Wbudowany układ stabilizacji napięcia AVR Funkcja „zimny start”
Gniazda	Min. 2 gniazda wyjściowe AC pozwalające na podtrzymanie zasilania zestawu komputerowego (jednostka + monitor). Jeśli jest wymagane dodatkowe okablowanie nie będące podstawowym wyposażeniem zasilacza, to jego zapewnienie leży po stronie Wykonawcy.
Gwarancja i serwis	Min. 2 lata (24 miesiące)

16. Zakup zasilaczy awaryjnych UPS do punktów pośrednich sieci

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	2 sztuki dla jednostki organizacyjnej: Urząd Miejski
Obudowa	Typu Rack o wysokości min. 1U wyposażona w graficzny wyświetlacz LCD
Klasa	Line-interactive
Moc pozorna	min. 800VA
Kształt napięcia	Sinusoida
Funkcjonalności	Wbudowany układ stabilizacji napięcia AVR Funkcja „zimny start”
Gniazda	Min. 2 gniazda wyjściowe AC pozwalające na podtrzymanie zasilania przełączników sieciowych. Jeśli jest wymagane dodatkowe okablowanie nie będące podstawowym wyposażeniem zasilacza, to jego zapewnienie leży po stronie Wykonawcy.
Gwarancja i serwis	Min. 2 lata (24 miesiące)

17. Zakup zarządzalnych przełączników sieciowych (typ 1)

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia



Cyberbezpieczny Samorząd

Ilość	2 sztuki dla jednostki organizacyjnej: Urząd Miejski
Obudowa	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack.
Parametry fizyczne	<ul style="list-style-type: none">▪ możliwość montażu w stelażu/szafie 19"▪ wysokość maksymalna 1U▪ wewnętrzny zasilacz 230V AC▪ port USB umożliwiający podłączenie zewnętrznej pamięci flash▪ ochrona przed przepięciami: minimum ± 6 kV▪ MTBF: minimum 30 lat
Porty	<ul style="list-style-type: none">▪ 48x 100M/1000M Base-T RJ45 PoE+▪ 4x 1G/10G SFP+▪ 2x dedykowane porty do zestawiania stosu
Stos	Przełącznik musi umożliwiać łączenie w stos z zachowaniem następującej funkcjonalności: <ul style="list-style-type: none">▪ zarządzanie stosem poprzez jeden adres IP,▪ do min. 9 jednostek w stosie,▪ możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation),▪ stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree.
Wydajność, obsługa ruchu sieciowego	<ul style="list-style-type: none">▪ Układ przełączający o wydajności min. 224 Gbps, wydajność przełączania przynajmniej 168 Mpps▪ Obsługa min. 32000 adresów MAC▪ Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)▪ Wsparcie dla funkcji VLAN slicing▪ Możliwość skonfigurowania min. 1024 interfejsów vlan interface SVI działających równocześnie▪ Obsługa ramek jumbo o wielkości min. 9216 bajtów▪ Obsługa Multicast PIM DM, PIM SM, PIM SSM▪ Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree, ERPS (G.8032)▪ Obsługa min. 4096 tras dla routingu IPv4▪ Obsługa min. 1024 tras dla routingu IPv6



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Obsługa protokołów routingu▪ Static route, RIP, RIPng, OSPF, OSPFv3, VRRP, VRRP6, Routing Policy, Policy-Based Routing.▪ Obsługa wirtualnych tablic routingu-forwardingu (VRF) min 64 instancje.▪ Obsługa protokołów LLDP i LLDP-MED▪ Przełącznik musi posiadać funkcjonalność DHCP Server▪ Obsługa ruchu multicast: IGMP v1, v2 i v3; IGMP Snooping v1, v2 i v3; MLD Snooping <p>Wymagana implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:</p> <ul style="list-style-type: none">▪ Obsługa mechanizmów: PQ, PQ+WDRR, WRR oraz PQ+WRR▪ 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. <p>Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.</p>
Bezpieczeństwo sieci	<ul style="list-style-type: none">▪ min. 4 poziomy dostępu administracyjnego poprzez konsolę▪ autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL▪ możliwość utworzenia minimum 2000 list ACL▪ możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www▪ zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6▪ możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP▪ obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny),





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ możliwość synchronizacji czasu zgodnie z NTP▪ obsługa funkcjonalności DLDP lub równoważnej
Pozostałe wymagania	<ul style="list-style-type: none">▪ System operacyjny (firmware) musi być dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.▪ Wbudowana pamięć RAM min. 2GB.▪ Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1GB.▪ Wymagana 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▪ 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).▪ Urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych.▪ Dedykowany port konsoli (RJ45).
Gwarancja i serwis	Min. 2 lata (24 miesiące)
Warunki gwarancji	<ul style="list-style-type: none">▪ Możliwość zgłaszania błędów 24/7 telefonicznie za pomocą email lub poprzez stronę producenta.▪ Wymagane dostarczenie części zamiennych w trybie 9x5xNBD.▪ Wymagany bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.

18. Zakup zarządzalnych przełączników sieciowych (typ 2)

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	2 sztuki dla jednostki organizacyjnej: Miejski Ośrodek Pomocy Społecznej
Cechy sprzętowe	<ul style="list-style-type: none">▪ Urządzenie musi być wyposażone w min. 24 gigabitowe porty PoE+ na wtyk RJ45 oraz min. cztery 10-cio gigabitowe porty SFP+





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Urządzenie musi być wyposażone w port konsoli umożliwiający zarządzanie urządzeniem z poziomu linii komend▪ Rozmiar tablicy adresów MAC urządzenia min. 16K▪ Min. przepustowość urządzenia - 128 Gbps▪ Min. szybkość przekierowań pakietów - 95,2 Mpps▪ Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19" oraz posiadać w zestawie odpowiednie uchwyty montażowe
Standardy	Urządzenie musi spełniać następujące standardy: <ul style="list-style-type: none">▪ 802.3x▪ 802.3ad▪ 802.1ab▪ 802.1d▪ 802.1w▪ 802.1s▪ 802.1p▪ 802.1q
Gwarancja i serwis	Min. 2 lata (24 miesiące)

19. Zakup Access Point (typ 1)

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	10 sztuk dla jednostki organizacyjnej: Urząd Miejski
Cechy sprzętowe, właściwości transmisji, zarządzanie	<ol style="list-style-type: none">1. Urządzenie musi być wyposażone port RJ45 oraz pasywne zasilanie PoE.2. Urządzenie musi być wyposażone w przycisk przywracania ustawień.3. Urządzenie musi być wyposażone w min 4 anteny wewnętrzne dookólne o zysku min 4dBi dla sieci 2,4GHz oraz min 5dBi dla sieci 5GHz.4. Urządzenie musi pracować w standardzie IEEE 802.11ax (WiFi 6) /ac (WiFi5) /n (WiFi4) / g / b /a oraz częstotliwości pracy 2,4 oraz 5 GHz.5. Urządzenie powinno być dostosowane do montażu na ścianie lub suficie oraz posiadać dołączony zestaw montażowy.



Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">6. Urządzenie musi pracować zarówno jako urządzenie typu stand-alone lub w trybie podłączonym do kontrolera sieci bezprzewodowej.7. Kontroler sieci bezprzewodowej realizowany musi być jako oprogramowanie przeznaczone do instalacji na systemach operacyjnych Windows/Linux lub kontroler sprzętowy - oddzielne urządzenie.8. Oprogramowanie kontrolera sieci bezprzewodowych musi być realizowane jako oprogramowanie bezpłatne, bez dodatkowych opłat licencyjnych.
Gwarancja i serwis	Min. 2 lata (24 miesiące)

20. Zakup Access Point (typ 2)

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	4 sztuki dla jednostki organizacyjnej: Miejski Ośrodek Pomocy Społecznej
Cechy sprzętowe, właściwości transmisji, zarządzanie	<ol style="list-style-type: none">1. Urządzenie musi być wyposażone port RJ45 oraz pasywne zasilanie PoE.2. Urządzenie musi być wyposażone w przycisk przywracania ustawień3. Urządzenie musi być wyposażone w min 2 anteny wewnętrzne dookólne o zysku min 4dBi dla sieci 2,4GHz oraz min 5dBi dla sieci 5GHz4. Urządzenie musi pracować w standardzie IEEE 802.11ax (WiFi 6) /ac (WiFi5) /n (WiFi4) / g / b / a oraz częstotliwości pracy 2,4 oraz 5 GHz5. Urządzenie powinno być dostosowane do montażu na ścianie lub suficie oraz posiadać dołączony zestaw montażowy6. Urządzenie musi pracować zarówno jako urządzenie typu stand-alone lub w trybie podłączonym do kontrolera sieci bezprzewodowej7. Kontroler sieci bezprzewodowej realizowany musi być jako oprogramowanie przeznaczone do instalacji na systemach operacyjnych Windows/Linux lub kontroler sprzętowy - oddzielne urządzenie8. Oprogramowanie kontrolera sieci bezprzewodowych musi być realizowane jako oprogramowanie bezpłatne, bez dodatkowych opłat licencyjnych.
Gwarancja i serwis	Min. 2 lata (24 miesiące)





Cyberbezpieczny Samorząd

21. Zakup dysków zewnętrznych USB w celu przechowywania odseparowanych od sieci kopii zapasowych

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	8 sztuk dla jednostki organizacyjnej: Urząd Miejski
Pojemność	5TB
Złącze	USB 3.2 Gen. 1
Bezpieczeństwo	256-bitowe szyfrowanie danych AES Ochrona danych za pomocą klucza dostępu
Gwarancja i serwis	Min. 2 lata (24 miesiące)

22. Zakup urządzenia klasy UTM (typ 1) do budowy klastra HA wraz z licencjami i wsparciem technicznym w okresie realizacji projektu

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	1 zestaw dla jednostki organizacyjnej: Urząd Miejski
Wymagania ogólne	Dostarczone urządzenie klasy UTM musi umożliwić budowę klastra wysokiej dostępności HA z urządzeniem posiadanym przez Zamawiającego, tj. FortiGate-80F i 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.



Cyberbezpieczny Samorząd

	<p>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.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none">▪ Firewall.▪ Ochrony w warstwie aplikacji.▪ Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none">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:	<ol style="list-style-type: none">1. System realizujący funkcję Firewall musi dysponować minimum:<ul style="list-style-type: none">▪ 10 portami Gigabit Ethernet RJ-45.▪ 2 gniazdami SFP 1 Gbps.2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych definiowanych jako VLAN'y w oparciu o standard 802.1Q.4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	<ol style="list-style-type: none">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 protokołem AES z kluczem 128 nie mniej niż 6 Gbps.



Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,3 Gbps.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
Funkcje Systemu Bezpieczeństwa	<p>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:</p> <ol style="list-style-type: none">1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.2. Kontrola Aplikacji.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.4. Ochrona przed malware.5. Ochrona przed atakami - Intrusion Prevention System.6. Kontrola stron WWW.7. Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3.8. Zarządzanie pasmem (QoS, Traffic shaping).9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.13. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).





Cyberbezpieczny Samorząd

Polityki, Firewall	<ol style="list-style-type: none">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:<ul style="list-style-type: none">▪ Translację jeden do jeden oraz jeden do wielu.▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP.3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.4. Wymagana możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.5. Polityka firewall umożliwiającą filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.6. Wymagana możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.7. 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.<ul style="list-style-type: none">▪ Amazon Web Services (AWS).▪ Microsoft Azure.▪ Cisco ACI.▪ Google Cloud Platform (GCP).▪ OpenStack.▪ VMware NSX.▪ Kubernetes.
Połączenia VPN	<ol style="list-style-type: none">1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:<ul style="list-style-type: none">▪ Wsparcie dla IKE v1 oraz v2.▪ Obsługę szyfrowania protokołem minimum AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM).▪ Obsługę protokołu Diffie-Hellman grup 19, 20.▪ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.▪ Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.▪ Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.▪ Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.▪ Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.▪ Mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:</p> <ul style="list-style-type: none">▪ 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. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <ol style="list-style-type: none">1. Routingu statycznego.2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.6. BFD (Bidirectional Forwarding Detection).





Cyberbezpieczny Samorząd

	7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	<ol style="list-style-type: none">1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.2. SD-WAN musi wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	<ol style="list-style-type: none">1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.2. System musi dać możliwość określania pasma dla poszczególnych aplikacji.3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.4. System musi zapewnić możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	<ol style="list-style-type: none">1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych musi istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.5. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.8. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.





Cyberbezpieczny Samorząd

	<p>9. System musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>10. Wymagana możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p>
Ochrona przed atakami	<p>1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>2. System ma chronić przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>6. Wymagane mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>7. Wymagana możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</p> <p>8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>9. Wymagana możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie</p>
Kontrola aplikacji	<p>1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p>





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.6. Wymagana możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).7. System musi umożliwiać określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola www	<ol style="list-style-type: none">1. Moduł kontroli WWW powinien 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 powinien dostarczać kategorii stron zabronionych prawem np.: Hazard.4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).6. Filtr WWW ma dawać możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.7. Wymagana Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.8. Administrator ma mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none">1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:<ul style="list-style-type: none">▪ Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.▪ Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <ol style="list-style-type: none">2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http.
Zarządzanie	<ol style="list-style-type: none">1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania ma być realizowana z wykorzystaniem szyfrowanych protokołów.3. Musi istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.5. System musi dać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.6. Element systemu pełniący funkcję Firewall 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.8. Wymagana możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).9. Wymagana możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.





Cyberbezpieczny Samorząd

Logowanie	<ol style="list-style-type: none">1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach dostawy musi zostać zapewniony (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. <u>Zamawiający wymaga zapewnienia tej funkcjonalności w okresie realizacji projektu, tj. nie dłużej niż do 30.06.2026 r.</u>3. 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.4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.5. Musi istnieć możliwość logowania do serwera SYSLOG.6. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.7. Wymagana możliwość włączenia logowania per reguła w polityce firewall.8. System musi zapewniać możliwość logowania do serwera SYSLOG.9. Przesyłanie SYSLOG do zewnętrznych systemów będzie możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Test funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	<p>W ramach realizacji zadania Zamawiający wymaga dostarczenia licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. <u>Zamawiający wymaga zapewnienia tej funkcjonalności w okresie realizacji projektu, tj. nie dłużej niż do 30.06.2026 r.</u></p> <p>Powinny one obejmować:</p> <ol style="list-style-type: none">1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),





Cyberbezpieczny Samorząd

	<p>Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.</p> <p>2. Licencja na usługę realizowaną w chmurze umożliwiającą logowanie i raportowanie z czasem retencji logów.</p>
Gwarancja i serwis	Min. 2 lata (24 miesiące)
Warunki gwarancji	<ul style="list-style-type: none">System musi być objęty serwisem gwarancyjnym, 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.
Wsparcie techniczne dla systemu Firewall	<p>Zamawiający wymaga dostawy systemu objętego rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres udzielonej gwarancji.</p> <p>Dla dostarczonego rozwiązania Wykonawca zapewni usługę wsparcia technicznego świadczoną w języku polskim przez producenta lub Autoryzowanego Partnera Serwisowego Producenta w okresie udzielonej gwarancji <u>w okresie realizacji projektu, tj. nie dłużej niż do 30.06.2026</u> co najmniej w następującym zakresie:</p> <ul style="list-style-type: none">wsparcie telefoniczne zespołu certyfikowanych inżynierów,pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu,doradztwo w zakresie konfiguracji,zdalne wsparcie techniczne,pomoc w zakładaniu zgłoszeń serwisowych u producenta,pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta,przygotowanie urządzenia do zdalnej konfiguracji,zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika,minimum 5 (pięć) zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika,





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ minimum 2 (dwa) razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich▪ minimum 2 (dwa) razy w roku zdalny upgrade oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich <p>Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wymagany czas reakcji nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym</p>
Pozostałe wymagania	<ol style="list-style-type: none">1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

23. Zakup utrzymania wsparcia technicznego wraz z subskrypcjami w okresie realizacji projektu dla posiadanego UTM

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania





Cyberbezpieczny Samorząd

Ilość	1 zestaw dla jednostki organizacyjnej: Urząd Miejski
Rodzaj wsparcia z subskrypcjami	<p>W celu zapewnienia pełnej ochrony sieci wewnętrznej Urzędu Miejskiego, Zamawiający wymaga dostarczenia pakietów licencji dotyczących wsparcia technicznego wraz z subskrypcjami dla wymienionych funkcji bezpieczeństwa powiązanych z posiadanym urządzeniem FortiGate-80F:</p> <ol style="list-style-type: none">1. <i>Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)</i>2. <i>Cloud Management, Analysis and Log Retention</i>3. <i>HEZO 360</i> <p>Licencje oraz serwisy powinny mieć zapewnione wsparcie techniczne oraz subskrypcję na okres 2 lat (24 miesięcy), w okresie realizacji projektu, lecz nie dłużej niż do 30.06.2026 r.</p>

24. Zakup utrzymania wsparcia technicznego wraz z subskrypcjami dla posiadanego oprogramowania do realizacji kopii zapasowych w okresie realizacji projektu

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania
Ilość	1 zestaw dla jednostki organizacyjnej: Urząd Miejski
Rodzaj wsparcia z subskrypcjami	<p>Przedmiotem zadania jest dostawa aktualizacji wsparcia technicznego wraz z subskrypcjami dla posiadanej licencji do realizacji kopii zapasowych pod nazwą „<i>Veeam Backup Essentials Universal Perpetual License. Includes Enterprise Plus Edition features.</i>”</p> <p>Licencje oraz serwisy powinny mieć zapewnione wsparcie techniczne oraz subskrypcję na okres 2 lat (24 miesięcy), w okresie realizacji projektu, lecz nie dłużej niż do 30.06.2026 r.</p> <p>Liczba licencji posiadanych przez Zamawiającego = 2.</p>

25. Zakup licencji oprogramowania do realizacji kopii zapasowych ze wsparciem w okresie realizacji projektu

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny





Cyberbezpieczny Samorząd

Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania
Ilość	1 zestaw dla jednostki organizacyjnej: Urząd Miejski
Wymagania ogólne	<ol style="list-style-type: none">1. Oprogramowanie musi zapewnić realizację kopii zapasowych z 2 (dwóch) serwerów fizycznych i 8 (ośmiu) maszyn wirtualnych.2. Licencje oraz serwisy powinny mieć zapewnione wsparcie techniczne oraz subskrypcję w okresie realizacji projektu, lecz nie dłużej niż do 30.06.2026 r.3. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.4. 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	<ol style="list-style-type: none">1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.2. Oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.3. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji4. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.6. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z





Cyberbezpieczny Samorząd

	<p>S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.</p> <ol style="list-style-type: none">7. Oprogramowanie musi wspierać niezmiennność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji13. 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 specyfikacji14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej17. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)18. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)19. Oprogramowanie musi posiadać integracje z systemami typu SIEM
--	---





Cyberbezpieczny Samorząd

	<p>20. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.</p>
Wymagania RPO	<ol style="list-style-type: none">1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.9. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Wymagania RTO	<ol style="list-style-type: none">1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie 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 mechanizmami4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere





Cyberbezpieczny Samorząd

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





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.17. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.19. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db224. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Ograniczenie ryzyka	<ol style="list-style-type: none">1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację





Cyberbezpieczny Samorząd

	<p>uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem</p> <ol style="list-style-type: none">Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malwareOprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowaniaOprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberatakówOprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Środowiska fizyczne	<ol style="list-style-type: none">Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnegoRozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowychRozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSERozwiązanie musi wspierać system operacyjny macOSOprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, UnixRozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)Rozwiązanie musi wspierać systemy oparte o Microsoft Failover ClusterRozwiązanie 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





Cyberbezpieczny Samorząd

9. Rozwiązanie musi wspierać backup podłączonych dysków USB
10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
12. Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
13. Rozwiązanie musi wspierać kontrolę pasma sieciowego
14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
17. Rozwiązanie musi wspierać technologię BitLocker
18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednorazowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
22. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
23. Rozwiązanie musi wspierać szyfrowanie





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
Monitoring	<ul style="list-style-type: none">1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.4. System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel7. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna12. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.15. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware17. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4
Raportowanie	<ol style="list-style-type: none">1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie2. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.3. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych11. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta13. 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 nadanych użytkownikom dla platformy VMware16. 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
--	---





Cyberbezpieczny Samorząd

26. Zakup urządzenia klasy UTM (typ 2) wraz z licencjami i wsparciem technicznym w okresie realizacji projektu

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	1 zestaw dla jednostki organizacyjnej: Miejski Ośrodek Pomocy Społecznej
Wymagania ogólne	<p>Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.</p> <p>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.</p> <p>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none">▪ Firewall.▪ Ochrony w warstwie aplikacji.▪ Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none">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.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.



Cyberbezpieczny Samorząd

Interfejsy, Zasilanie:	<ol style="list-style-type: none">1. System realizujący funkcję Firewall musi dysponować minimum 5 portami Gigabit Ethernet RJ-45.2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych definiowanych jako VLAN'y w oparciu o standard 802.1Q.4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	<ol style="list-style-type: none">1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950Mbps.4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - minimum 300 Mbps.
Funkcje Systemu Bezpieczeństwa	<p>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:</p> <ol style="list-style-type: none">1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.2. Kontrola Aplikacji.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.4. Ochrona przed malware.5. Ochrona przed atakami - Intrusion Prevention System.6. Kontrola stron WWW.7. Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3.8. Zarządzanie pasmem (QoS, Traffic shaping).



Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">9. Mechanizmy ochrony przed wyciekami 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.13. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomienia do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	<ol style="list-style-type: none">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:<ul style="list-style-type: none">▪ Translację jeden do jeden oraz jeden do wielu.▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP.3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.4. Wymagana możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.5. Polityka firewall umożliwiająca filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.6. Wymagana możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.7. 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.<ul style="list-style-type: none">▪ Amazon Web Services (AWS).





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Microsoft Azure.▪ Cisco ACI.▪ Google Cloud Platform (GCP).▪ OpenStack.▪ VMware NSX.▪ Kubernetes.
Połączenia VPN	<ol style="list-style-type: none">1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:<ul style="list-style-type: none">▪ Wsparcie dla IKE v1 oraz v2.▪ Obsługę szyfrowania protokołem minimum AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM).▪ Obsługę protokołu Diffie-Hellman grup 19, 20.▪ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.▪ Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.▪ Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.▪ Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.▪ Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.▪ Mechanizm „Split tunneling” dla połączeń Client-to-Site.2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:<ul style="list-style-type: none">▪ 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.





Cyberbezpieczny Samorząd

	Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <ol style="list-style-type: none">1. Routingu statycznego.2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.6. BFD (Bidirectional Forwarding Detection).7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	<ol style="list-style-type: none">1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.2. SD-WAN musi wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	<ol style="list-style-type: none">1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.2. System musi dać możliwość określania pasma dla poszczególnych aplikacji.3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.4. System musi zapewnić możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	<ol style="list-style-type: none">1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych musi istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.5. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.8. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.9. System musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.10. Wymagana możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	<ol style="list-style-type: none">1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.2. System ma chronić przed atakami na aplikacje pracujące na niestandardowych portach.3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i musi 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. Wymagane mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">7. Wymagana możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.9. Wymagana możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie
Kontrola aplikacji	<ol style="list-style-type: none">1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.6. Wymagana możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).7. System musi umożliwiać określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola www	<ol style="list-style-type: none">1. Moduł kontroli WWW powinien 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 powinien dostarczać kategorii stron zabronionych prawem np.: Hazard.4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).6. Filtr WWW ma dawać możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.7. Wymagana Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.8. Administrator ma mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none">1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:<ul style="list-style-type: none">▪ Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.▪ Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.▪ Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http.
Zarządzanie	<ol style="list-style-type: none">1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania ma być realizowana z wykorzystaniem szyfrowanych protokołów.





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">3. Musi istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.5. System musi dać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.6. Element systemu pełniący funkcję Firewall 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.8. Wymagana możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).9. Wymagana możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	<ol style="list-style-type: none">1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach dostawy musi zostać zapewniony (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. <u>Zamawiający wymaga zapewnienia tej funkcjonalności w okresie realizacji projektu, tj. nie dłużej niż do 30.06.2026 r.</u>3. 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.4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.5. Musi istnieć możliwość logowania do serwera SYSLOG.





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">6. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.7. Wymagana możliwość włączenia logowania per reguła w polityce firewall.8. System musi zapewniać możliwość logowania do serwera SYSLOG.9. Przesyłanie SYSLOG do zewnętrznych systemów będzie możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Test funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	<p>W ramach realizacji zadania Zamawiający wymaga dostarczenia licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. <u>Zamawiający wymaga zapewnienia tej funkcjonalności w okresie realizacji projektu, tj. nie dłużej niż do 30.06.2026 r.</u></p> <p>Powinny one obejmować:</p> <ol style="list-style-type: none">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 umożliwiającą logowanie i raportowanie z czasem retencji logów.
Gwarancja i serwis	Min. 2 lata (24 miesiące)
Warunki gwarancji	<ul style="list-style-type: none">▪ System musi być objęty serwisem 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.
Pozostałe wymagania	<ol style="list-style-type: none">1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system





Cyberbezpieczny Samorząd

	<p>zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.</p> <p>2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.</p>
--	---

27. Zakup serwera (typ 2) z systemem operacyjnym

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
Ilość	Łącznie 2 zestawy dla jednostek organizacyjnych: <ul style="list-style-type: none">▪ Miejski Ośrodek Pomocy Społecznej - 1 zestaw▪ Zespół Obsługi Placówek Oświatowych - 1 zestaw
Funkcjonalność obudowy	<ul style="list-style-type: none">▪ Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków Hot-Plug, wraz z kompletem wysuwanych szyn umożliwiającym montaż w szafie Rack i wysuwanie serwera do celów serwisowych.▪ Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Funkcjonalność płyty głównej	Min.: 4 sloty pamięci RAM
Procesor	<p>Jeden procesor wielordzeniowy dedykowany do pracy z zaoferowanym serwerem umożliwiającym osiągnięcie wyniku min. 95 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org</p> <p><i>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.</i></p>
Pamięć RAM	128 GB pamięci RAM





Cyberbezpieczny Samorząd

Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none">▪ 2 porty 1Gb Ethernet w standardzie BaseT▪ 2 porty 10Gb Ethernet w standardzie BaseT
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none">▪ Min. 8GB nieulotnej pamięci cache,▪ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.▪ Wsparcie dla dysków samoszyfrujących.
Dyski twarde	Zainstalowane: <ul style="list-style-type: none">▪ 2 dyski Hot-Plug M.2 NVMe SSD o pojemności min. 480GB każdy z możliwością konfiguracji RAID 1▪ 8 dysków Hot-Plug SAS o pojemności min. 1.2TB każdy
Porty/złącza	<ul style="list-style-type: none">▪ 4x USB, w tym co najmniej 1x USB 3.0▪ VGA▪ RS232
Karta graficzna	Karta graficzna umożliwiająca pracę w rozdzielczości 1920x1200
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz o mocy max. 700W klasy Titanium (1+1)
Bezpieczeństwo	<ul style="list-style-type: none">▪ Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.▪ Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.▪ Moduł TPM 2.0▪ Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta zarządzająca	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: <ul style="list-style-type: none">▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);▪ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;▪ możliwość podmontowania zdalnych wirtualnych napędów;▪ wirtualną konsolę z dostępem do myszy, klawiatury;



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ wsparcie dla IPv6;▪ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;▪ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;▪ integracja z Active Directory;▪ możliwość obsługi przez dwóch administratorów jednocześnie;▪ wsparcie dla dynamic DNS;▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.▪ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera▪ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none">▪ wirtualny schowek ułatwiający korzystanie z konsoli zdalnej;▪ przesyłanie danych telemetrycznych w czasie rzeczywistym; dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze;▪ automatyczna rejestracja certyfikatów (ACE).
Oprogramowanie do zarządzania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none">▪ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych▪ Integracja z Active Directory▪ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta▪ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish▪ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram▪ Szczegółowy opis wykrytych systemów oraz ich komponentów▪ Możliwość eksportu raportu do CSV, HTML, XLS, PDF▪ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.▪ Grupowanie urządzeń w oparciu o kryteria użytkownika





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji▪ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach▪ Szybki podgląd stanu środowiska▪ Podsumowanie stanu dla każdego urządzenia▪ Szczegółowy status urządzenia/elementu/komponentu▪ Generowanie alertów przy zmianie stanu urządzenia.▪ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń▪ Integracja z service desk producenta dostarczonej platformy sprzętowej▪ Możliwość przejęcia zdalnego pulpitu▪ Możliwość podmontowania wirtualnego napędu▪ Kreator umożliwiający dostosowanie akcji dla wybranych alertów▪ Możliwość importu plików MIB▪ Przesyłanie alertów „as-is” do innych konsol firm trzecich▪ Możliwość definiowania ról administratorów▪ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów▪ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)▪ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta▪ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów▪ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.▪ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.▪ Wdrażanie serwerów, rozwiązań modułarnych oraz przełączników sieciowych w oparciu o profile
--	--





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.Zdalne uruchamianie diagnostyki serwera.Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Gwarancja i serwis	Min. 2 lata (24 miesiące)
Warunki gwarancji	<ul style="list-style-type: none">Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych)Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej/ internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.Zamawiający wymaga gwarancji uwzględniającej zabezpieczenie serwisowe, które w przypadku awarii dysku twardego (w urządzeniu objętym aktywnym





Cyberbezpieczny Samorząd

	<p>wparciem technicznym) powodującej konieczność jego wymiany, umożliwi pozostawienie uszkodzonego dysku u Zamawiającego (dysk nie będzie podlegał ekspertyzie poza siedzibą Zamawiającego).</p> <ul style="list-style-type: none">▪ Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocenę bezpieczeństwa cybernetycznego.▪ Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń.
Certyfikaty, normy i standardy	<ul style="list-style-type: none">▪ Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie produkcji - <i>dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</i>▪ Spełnienie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie produkcji - <i>dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</i>▪ Spełnienie normy ISO 50001 lub równoważnej dla producenta sprzętu w zakresie produkcji - <i>dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</i>▪ Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.▪ Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows Server 2019, Microsoft Windows Server 2022.▪ Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich





Cyberbezpieczny Samorząd

	<p>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.</p> <p><i>Dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku.</i></p>
System operacyjny	<p>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.</p> <p>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.</p> <ol style="list-style-type: none">1. Możliwość wykorzystania 128GB 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:<ol style="list-style-type: none">a) pozwalają na zmianę rozmiaru w czasie pracy systemu,b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).5. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.6. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agencję rządową zajmującą się bezpieczeństwem informacji.





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">7. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET8. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.9. Wbudowana zaporą internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.10. Dostępne dwa rodzaje graficznego interfejsu użytkownika:<ol style="list-style-type: none">a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,b) dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.11. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,12. Mechanizmy logowania w oparciu o:<ol style="list-style-type: none">a) Login i hasło,b) Karty z certyfikatami (smartcard),c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),13. 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.14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).15. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.16. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.17. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).18. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.19. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:<ol style="list-style-type: none">a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
--	---





Cyberbezpieczny Samorząd

	<p>b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:</p> <ul style="list-style-type: none">▪ Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,▪ Ustawianie 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. <p>c) Zdalna dystrybucja oprogramowania na stacje robocze.</p> <p>d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej</p> <p>e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:</p> <ul style="list-style-type: none">▪ 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. <p>f) Szyfrowanie plików i folderów.</p> <p>g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</p> <p>h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.</p> <p>i) Serwis udostępniania stron WWW.</p> <p>j) Wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>k) Wsparcie dla algorytmów Suite B (RFC 4869),</p>
--	--





Cyberbezpieczny Samorząd

	<p>1) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,</p> <p>20. 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.</p> <p>21. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p>
--	--

Atrybut	Wymagania <i>dodatkowe</i> (fakultatywne, nieobowiązkowe)
Uszczegółowienie	Za spełnienie wymagania dodatkowego Wykonawcy zostanie przyznana liczba punktów określona w pozostałych kryteriach oceny ofert zgodnie z kryteriami określonymi w rozdziale 16 SWZ.
Dodatkowy okres gwarancji (wymaganie nieobowiązkowe)	<p>Zaoferowanie serwerów z dodatkową gwarancją udzieloną przez producenta lub gwarancją udzieloną przez autoryzowany serwis producenta serwerów 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 serwerów z systemem operacyjnym - typ 2 (S2).</p> <p>W przypadku zaoferowania gwarancji wydłużającej gwarancję podstawową, okres zabezpieczenia serwisowego na nośniki pamięci masowej (dyski twarde), musi być tożsamy z czasem gwarancji udzielonej na serwery po wydłużeniu gwarancji podstawowej.</p> <p><u>Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.</u></p>

28. Zakup serwera NAS (typ 2) z dyskami

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Techniczny
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia





Cyberbezpieczny Samorząd

Ilość	Łącznie 2 zestawy dla jednostek organizacyjnych: <ul style="list-style-type: none">▪ Miejski Ośrodek Pomocy Społecznej - 1 zestaw▪ Zespół Obsługi Placówek Oświatowych - 1 zestaw
Funkcjonalność obudowy	<ul style="list-style-type: none">▪ Do instalacji w standardowej szafie typu Rack 19", serwer musi zajmować maksymalnie wysokość 1U, w zestawie szyny do montażu serwera w szafie typu Rack.▪ Możliwość obsługi (instalacji) 4 dysków.▪ Wyposażona w gniazda: 2x USB 3.2 Gen 1, 1x eSATA
Procesor	Wymagany procesor wielordzeniowy, umożliwiający osiągnięcie w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik min. 5000 punktów. <i>Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony www.cpubenchmark.net</i>
Pamięć	<ul style="list-style-type: none">▪ Pamięć RAM: 16 GB z możliwością rozbudowy do 32GB▪ Pamięć masowa: dyski twarde klasy Enterprise przystosowane do zapisu ciągłego, kompatybilne z oferowanym urządzeniem, 4 sztuki o pojemności 6TB każdy.
System plików	<ul style="list-style-type: none">▪ Wewnętrzny: Btrfs, ext4▪ Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
RAID	Obsługiwane typy macierzy RAID: SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Bezpieczeństwo	Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Protokoły	SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Interfejsy sieciowe	<ul style="list-style-type: none">▪ 4 porty Gigabit sieci Ethernet (RJ45) z obsługą funkcji Link Aggregation▪ 2 porty SFP+
Dołączone oprogramowanie	<ul style="list-style-type: none">▪ Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych.▪ Oprogramowanie zarządzające serwerem NAS musi zapewnić nieodpłatne, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla



Cyberbezpieczny Samorząd

	<p>heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów.</p> <ul style="list-style-type: none">• Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń, a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.• Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz (1+1).
Funkcja udostępniania plików	<ul style="list-style-type: none">▪ Liczba kont użytkowników: 2048▪ Liczba grup użytkowników: 256▪ Liczba udziałów: 512▪ Liczba jednoczesnych połączeń: 2000
Gwarancja i serwis	Min. 2 lata (24 miesiące)

29. Usługi konfiguracyjne pozwalające wdrożyć nowe rozwiązania informatyczne

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
---------	---



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Obszar	Techniczny
Jednostka organizacyjna	Urząd Miejski Miejski Ośrodek Pomocy Społecznej Zespół Obsługi Placówek Oświatowych
Założenia ogólne	<p>Celem prac jest przygotowanie środowiska teleinformatycznego w jednostkach organizacyjnych objętych projektem w oparciu o dostarczone rozwiązania sprzętowe i oprogramowanie.</p> <p>Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielami Zamawiającego. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia oraz umożliwi Wykonawcy dostęp do infrastruktury w ustalonym terminie w celu przygotowania procedur wdrożenia. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa.</p> <p>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.</p> <p>Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych.</p>
Montaż i fizyczne uruchomienie systemu	<p>Zamawiający wymaga zainstalowania dostarczonych urządzeń we wskazanych pomieszczeniach co najmniej w zakresie:</p> <ol style="list-style-type: none">1. Wniesienie, ustawienie i fizyczny montaż dostarczonych urządzeń szafach typu Rack.2. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.3. Podłączenie całości rozwiązania do infrastruktury Zamawiającego.4. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.5. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.6. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji - Wykonawca zapewni niezbędne okablowanie, m.in. patchordy miedziane (min. kat. 6 UTP) lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym.



Cyberbezpieczny Samorząd

	7. Po wykonaniu instalacji, wymagane jest przeprowadzenie testów sprawdzających poprawność instalacji i działania urządzeń.
Reorganizacja i porządkowanie	Po zapoznaniu się z architekturą sieciową urzędu i przedstawieniu Zamawiającemu schematu reorganizacji sieci (z uwzględnieniem istniejącego i dostarczanego sprzętu), Wykonawca przeprowadzi porządkowanie połączeń wewnętrznych.
Konfiguracja przełączników sieci LAN	<p>Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi urządzeniami sieciowymi. Przełączniki będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łączy danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego). Wykonawca przeprowadzi konfigurację dostarczanych przełączników w zakresie:</p> <ol style="list-style-type: none">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.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 oraz testowanie skuteczności zabezpieczeń.
Konfiguracja urządzeń klasy UTM	<ol style="list-style-type: none">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 gminy5. Konfiguracja dostarczonego systemu Firewall:<ol style="list-style-type: none">a. Konfiguracja podstawowych parametrówb. Konfiguracja translacji adresów NATc. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, serwery komunikacyjne telefonii IP, itp.d. Konfiguracja inspekcji określonych protokołów sieciowych;e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;g. Testowanie działania bramy <p>6. Konfiguracja modułów należących do systemu wykrywania włamań IPS:</p> <ul style="list-style-type: none">a. Konfiguracja podstawowych parametrówb. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;e. Testowanie działania ochrony IPS <p>7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.</p> <ul style="list-style-type: none">a. Przypisanie adresu IP do zarządzania.b. Konfiguracja inspekcji protokołów HTTP, SMTP, FTP, POP3c. Definicja reguł filtrowania/blokowania <p>8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej z uwierzytelnieniem w oparciu o usługę katalogową.</p> <p>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.</p> <p>10. W instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaze Zamawiający) dla każdej z poniższych funkcjonalności:</p> <ul style="list-style-type: none">a. kontrola dostępu - zaporę ogniową klasy Stateless Inspectionb. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rarc. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
--	---





Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)f. kontrola pasma oraz ruchu [QoS, Traffic shaping]g. Kontrola aplikacji oraz rozpoznawanie ruchu P2Ph. Ochrona przed wyciekiem poufnej informacji (DLP)i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL)j. Inspekcja ruchu SSLk. Ochrony przez atakami na stacje klienckiel. Kontrola pasma <p>11. Konfiguracja logowania i raportowania.</p> <p>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.</p> <p>13. Informacje uzupełniające:</p> <ul style="list-style-type: none">a) Urządzenia klasy UTM (typ 1) ma zostać użyte do budowy klastra HA z urządzeniem posiadanym przez urządb) urządzenia klasy UTM (typ 2) ma zostać uruchomione jako stand alone w Miejskim Ośrodek Pomocy Społecznej
Instalacja i konfiguracja serwerów, instalacja systemu operacyjnego	<p>Dla serwerów typ 1 i typ 2 wymagana konfiguracja odpowiedniego poziomu RAID uzgodniona z Zamawiającym.</p> <p>Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane, a następnie należy zainstalować niezbędne aktualizacje oraz poprawki udostępnione przez producenta systemu operacyjnego związane z bezpieczeństwem.</p>
Wirtualizacja dla serwerów typ 1	<p>Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w następującym zakresie:</p> <ul style="list-style-type: none">1. Aktywacja licencji oprogramowania wirtualizacyjnego2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego - aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.3. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach.4. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">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. 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 maszyn w liczbie uzgodnionej z Zamawiającym, w ilości na jakie pozwalają dostarczone licencje.9. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.10. Konfiguracja klastra wysokiej dostępności:<ol style="list-style-type: none">a. 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.b. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.c. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera.11. Weryfikacja działania klastra wysokiej dostępności.
Wirtualizacja dla serwerów typ 2	<p>Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego z wykorzystaniem serwera, co najmniej w następującym zakresie:</p> <ol style="list-style-type: none">1. Przygotowanie serwera do instalacji oprogramowania wirtualizacyjnego.2. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">3. Instalacja oprogramowania wirtualizacyjnego na instalowanym serwerze.4. Instalacja oprogramowania do zarządzania środowiskiem wirtualizacyjnym.5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.6. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.7. Przygotowanie koncepcji i wykonania wirtualizacji maszyn w liczbie uzgodnionej z Zamawiającym, w ilości na jakie pozwalają dostarczone licencje.8. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.9. Konfiguracji uprawnień w środowisku wirtualizacyjnym - integracja z usługą katalogową.
Usługa katalogowa	<p>Usługa katalogowa musi być uruchomiona na wskazanych przez Zamawiającego 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.</p> <p>Usługa powinna uwzględniać strukturę jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.</p> <p>Zalecane jest wdrożenie globalnej polityki haseł spełniających zasady złożoności - Szczegółowe dane zostaną przekazane na etapie konfiguracji.</p> <p>Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:</p> <ol style="list-style-type: none">1. Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości2. Śledzenie zmian dotyczących tworzenia, usuwania obiektów





Cyberbezpieczny Samorząd

	<p>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).</p>
Kopie zapasowe	<p>Instalacja oraz uruchomienie dostarczonego środowiska wykonywania kopii zapasowych (serwery NAS) oraz aktywacja wymaganych licencji.</p> <p>Wymagana będzie konfiguracja zadań wykonywania kopii zapasowych przy wykorzystaniu serwera NAS typ1 i oprogramowania do nich przypisanego:</p> <ol style="list-style-type: none">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). <p>Oprogramowanie musi umożliwiać:</p> <ol style="list-style-type: none">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). <p>Wymagana będzie konfiguracja zadań wykonywania kopii zapasowych przy wykorzystaniu serwerów NAS typ2 i oprogramowania do nich przypisanego:</p>





Cyberbezpieczny Samorząd

	<ol style="list-style-type: none">1. Instalacja oprogramowania do wykonywania kopii zapasowych.2. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:<ol style="list-style-type: none">a) kopie muszą być wykonywane na serwer NAS;b) kopie muszą być wykonywane automatycznie wg zadanego harmonogramu;c) kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;d) musi istnieć możliwość odtworzenia:<ul style="list-style-type: none">▪ całego systemu;▪ dysku serwera;▪ pojedynczych plików serwera3. Zdefiniowanie powiadomień o przebiegu wykonania kopii i zdarzeniach. <p>Uruchomione rozwiązania zostaną poddane testowaniu poprzez:</p> <ol style="list-style-type: none">1. Uruchomienie testowych zadań backupu.2. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień.3. Uruchomienie testowych zadań odtworzenia danych.
Szkolenie	<p>Wykonawca przeprowadzi w siedzibie Zamawiającego podstawowe szkolenie dla Administratorów systemu. Szkoleniem zostaną objęte osoby wskazane przez Zamawiającego z zakresie dostarczonego rozwiązania teleinformatycznego, co najmniej w zakresie:</p> <ol style="list-style-type: none">1. Obsługi dostarczonych serwerów, macierzy dyskowej oraz utrzymania klastra HA.2. Obsługi dostarczonego rozwiązania do backupu, archiwizacji danych oraz wykonywania kopii zapasowych.3. Zarządzania przełącznikami sieciowymi. <p>Celem szkolenia administratorów będzie zapoznanie się z systemem informatycznym, poznanie poszczególnych funkcji i modułów oraz nauka jego obsługi w praktyce. Wykonawca zobowiązany jest do przeprowadzenia szkoleń w formie instruktażu stanowiskowego dla personelu w podziale na role w Systemie</p>
Opracowanie dokumentacji	<p>Zamawiający wymaga opracowania dokumentacji technicznej użytkownika (dokumentacji powykonawczej) w formie papierowej i elektronicznej.</p>





Cyberbezpieczny Samorząd

technicznej, Odbiory	Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z dokumentacją.
-------------------------	---



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA