Załącznik nr 5 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Nazwa zamówienia:
„Cyberbezpieczny Samorząd”

Niniejszy dokument określa minimalne wymagania dla dostaw stanowiących przedmiot niniejszego postępowania. Dostarczony sprzęt musi być fabrycznie nowy (rok produkcji 2023/2024), nieużywany, wolny od wad oraz wolny od obciążeń prawami osób trzecich. Oferowany sprzęt musi być objęty gwarancją producenta i musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej. Zamawiający nie dopuszcza dostawy urządzeń odnawianych, demonstracyjnych czy powystawowych. W przypadku systemu operacyjnego dostarczone wraz ze sprzętem oprogramowanie musi być opatrzone we wszystkie atrybuty oryginalności i legalności, wymagane przez producenta oprogramowania w zależności od dostarczonej wersji.

Warunki dotyczące realizacji dostawy.

1. Wykonawca na swój koszt i ryzyko dostarczy przedmiot zamówienia, zgodny z wymaganiami przedstawionymi w niniejszym dokumencie.
2. Dostawę należy dostarczyć do siedziby Zamawiającego. Przez dostawę Wykonawca ma rozumieć sukcesywną lub jednorazową dostawę całego przedmiotu zamówienia do siedziby Zamawiającego a także rozładunek oraz wniesienie do wskazanego przez Zamawiającego pomieszczenia.
3. Wykonawca w cenie oferty uwzględni wszystkie koszty niezbędne do realizacji dostawy, m.in. rozładunek, wniesienie oraz utrzymanie porządku w czasie rozładunku prowadzonego na terenie urzędu.
4. 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.
5. 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.
6. Do czasu odbioru sprzętu przez Zamawiającego, ryzyko wszelkich niebezpieczeństw związanych z jego ewentualnym uszkodzeniem lub utratą ponosi Wykonawca.

7. Wraz ze sprzętem Wykonawca zobowiązany jest przekazać Zamawiającemu listę numerów seryjnych dostarczonych urządzeń wszelką dokumentację dostarczoną przez producenta sprzętu.
8. W ramach procedury odbioru, Zamawiający zastrzega sobie prawo do przeprowadzenia weryfikacji oryginalności i legalności zainstalowanego (dostarczonego) oprogramowania bezpośrednio u producenta oprogramowania, przed podpisaniem protokołu odbioru, w sposób który uzna za bezsporny. W przypadku wykrycia, że dostarczony system operacyjny lub inne dostarczone oprogramowanie jest nieoryginalny (nielegalny), nie jest nowy, był już używany lub był już wcześniej aktywowany, Zamawiający w takiej sytuacji odmówi przyjęcia sprzętu i wezwie Wykonawcę do usunięcia nieprawidłowości w wyznaczonym terminie.

Zamawiający wymaga zaoferowania usług oraz sprzętu spełniającego wymagania podstawowe i (lub) opcjonalnie wymagania dodatkowe **określone w niniejszym dokumencie**:

1. Obszar organizacyjny

1.1. Sporządzenie procedur i instrukcji SZBI, Wdrożenie SZBI

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Zakres usługi	Usługa oznacza opracowanie, dostarczenie oraz wdrożenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji, w tym obejmuje analizę, projektowanie, implementację i szkolenie związane z wdrożeniem SZBI w jednostce. Celem usługi jest zwiększenie ochrony danych i informacji w organizacji na poziomie technicznym oraz organizacyjnym, zapewnienie zgodności z obowiązującymi przepisami prawnymi oraz poprawę ogólnego poziomu bezpieczeństwa informacji. 1. Zamawiający wymaga, aby usługa opracowania dokumentacji oraz wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) została zrealizowana zgodnie ze standardem ISO/IEC 27001:2022. Usługa sporządzenia i wdrożenia SZBI będzie tworzona pod nadzorem Zamawiającego. 2. Obszar ciągłości działania - dostępności informacji powinien być zgodny z wymaganiami normy ISO 22301:2019 - na zasadzie „best effort”. 3. System powinien uwzględniać wdrożony system ochrony danych osobowych Zamawiającego. 4. Wdrożenie powinno zostać przeprowadzone zgodnie z metodyką płynnego zarządzania - Agile.

1.2. Audyt

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Zakres usługi	Zadanie obejmuje przeprowadzenie audytu wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy. 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-samorzad
Wymagania dla osoby	Audyt musi zostać przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. Wykaz certyfikatów wskazanych w w/w rozporządzeniu: 1. Certified Internal Auditor (CIA) 2. Certified Information System Auditor (CISA) 3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018r. poz. 650 i 1138), w zakresie certyfikacji osób; 4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób; 5. Certified Information Security Manager (CISM); 6. Certified in Risk and Information Systems Control (CRISC); 7. Certified in the Governance of Enterprise IT (CGEIT); 8. Certified Information Systems Security Professional (CISSP); 9. Systems Security Certified Practitioner(SSCP); 10. Certified Reliability Professional;

	11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert **Przed podpisaniem umowy Zamawiający będzie żądał przedłożenia przez Wykonawcę certyfikatu dla osoby wykonującej audyt (posiadającej uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu).**
Wymagania szczegółowe	Audyt musi zostać przeprowadzony w maksymalnym stopniu obiektywnie - poprzez przeprowadzone badania w urzędzie w celu przedstawienia rzeczywistego stanu audytowanego obszaru. Zamawiający zakłada, że Wykonawca przeznaczy nie mniej niż 2 dni robocze na wykonanie audytu w urzędzie na prowadzenie analiz do audytu w kontakcie z wskazanymi przez Zamawiającego pracownikami urzędu.
Raport	Dokument końcowy musi być podpisany przez osobę posiadającą uprawnienia (wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu). Raport z audytu należy dostarczyć do Urzędu Gminy w wersji elektronicznej oraz w wersji papierowej.

2. Obszar kompetencyjny

2.1. Szkolenia dla kadry pracowniczej z cyberbezpieczeństwa.

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Zakres usługi	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. Wymagana jest realizacja cyklu szkoleń w formie wykładu. 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. Zakres szkolenia: 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 postepowania w przypadku jego wystąpienia. 4. Podstawowe zasady bezpieczeństwa (bezpieczeństwo fizyczne): 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, 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.
Czas trwania	Minimum 2 godziny lekcyjne dla każdej grupy przy założeniu, że jedna godzina lekcyjna trwa 45 min.
Liczba uczestników	Wykonawca powinien skalkulować koszty organizacji szkoleń dla **16** uczestników.
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.

3. Obszar techniczny

3.1. Zakup serwera z systemem operacyjnym - 1 zestaw

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	1. W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania wraz z informacją o jego wyposażeniu zgodnie z wymaganiem formularza ofertowego. 2. W ofercie należy wskazać pełną nazwę handlową zaoferowanego procesora oraz należy wskazać pełną nazwę handlową zaoferowanego systemu operacyjnego.
Obudowa	1. Obudowa Rack o wysokości max 1U, wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych. 2. Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. 3. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy

	użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna wyposażona w: 1. 16 slotów pamięci RAM przeznaczonych do instalacji pamięci RAM, 2. Min. 3 sloty PCIe 3. Min. 2 gniazda (sockety) pod procesory, zapewniająca obsługę procesorów 32 rdzeniowych
Procesor / wydajność	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. *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.*
Pamięć RAM	256 GB pamięci RAM z możliwością rozbudowy do 1TB RAM. Wymagane funkcjonalności pamięci RAM: Demand Scrubing, Patrol Scrubing, Permanent Fault Detection.
Interfejsy sieciowe/FC/SAS	1. Interfejsy sieciowe 1GbE BaseT - min. 2 sztuki 2. Interfejsy sieciowe 10GbE BaseT - min. 2 sztuki
Dyski twarde	1. Zainstalowane 8 dysków Hot-plug SAS o pojemności min. 2,4TB. 2. Zainstalowane 2 dyski Hot-plug M.2 NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy umożliwiający konfigurację następujących poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
Porty / złącza	4x USB, w tym co najmniej 1x USB 3.0, 2x VGA
Karta graficzna	Karta graficzna umożliwiająca pracę w rozdzielczości 1920x1200
Zasilanie	Redundantne (1+1), Hot-Plug o mocy min 700W.
Bezpieczeństwo	1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

	3. BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. 4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5. Moduł TPM 2.0 6. Wymagana możliwość dynamicznego włączania i wyłączania portów USB na obudowie - bez potrzeby restartu serwera. 7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera - niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. 8. 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: 1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; 4. możliwość podmontowania zdalnych wirtualnych napędów; 5. wirtualną konsolę z dostępem do myszy, klawiatury; 6. wsparcie dla IPv6; 7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; 10. integracja z Active Directory; 11. możliwość obsługi przez dwóch administratorów jednocześnie;

	12. wsparcie dla dynamic DNS; 13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; 14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera; 15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera 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 rejestracja certyfikatów (ACE).
Oprogramowanie do zarządzania	Wymagana możliwość zainstalowania oprogramowania do zarządzania, spełniającego poniższe wymagania: 1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych. 2. Integracja z Active Directory. 3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta. 4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish. 5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram. 6. Szczegółowy opis wykrytych systemów oraz ich komponentów. 7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF. 8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. 9. Grupowanie urządzeń w oparciu o kryteria użytkownika. 10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji. 11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach. 12. Szybki podgląd stanu środowiska. 13. Podsumowanie stanu dla każdego urządzenia. 14. Szczegółowy status urządzenia/elementu/komponentu.

	15. Generowanie alertów przy zmianie stanu urządzenia. 16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń. 17. Integracja z service desk producenta dostarczonej platformy sprzętowej. 18. Możliwość przejęcia zdalnego pulpitu. 19. Możliwość podmontowania wirtualnego napędu. 20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów. 21. Możliwość importu plików MIB. 22. Przesyłanie alertów „as-is” do innych konsol firm trzecich. 23. Możliwość definiowania ról administratorów. 24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów. 25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania). 26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta. 27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów. 28. 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. 29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. 30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile. 31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. 32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. 33. Zdalne uruchamianie diagnostyki serwera. 34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

	35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty i standardy	1. Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie produkcji - *dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.* 2. Spełnienie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie produkcji - *dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.* 3. Spełnienie normy ISO 50001 lub równoważnej dla producenta sprzętu w zakresie produkcji - *dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.* 4. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. 5. 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. 6. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. - *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.*

Gwarancja	1. Wymagany minimalny okres gwarancji producenta to 2 lata (24 miesiące) 2. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. 3. 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) 4. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. 5. 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. 6. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 7. 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. 8. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 9. 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. 10. Serwis urządzeń będzie realizowany bezpośrednio przez producenta lub przez autoryzowany serwis producenta. Firma serwisująca musi posiadać ISO

	9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera.
Rozszerzenie gwarancji producenta **(wymaganie nieobowiązkowe)**	**Zaoferowanie serwera z dodatkową gwarancją realizowaną bezpośrednio przez producenta lub przez autoryzowany serwis producenta** wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36, 48 lub 60 miesięcy **jest wymogiem fakultatywnym** i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium „Gwarancja Serwera". W przypadku zaoferowania gwarancji wydłużającej gwarancję podstawową, okres zabezpieczenia serwisowego na dyski twarde, musi być równy gwarancji udzielonej na serwer po wydłużeniu gwarancji podstawowej. **Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.**
System operacyjny	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. Dostarczona licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym oraz nielimitowanej liczby 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, 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). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 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. 12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

	a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 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.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania

	dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: ▪ Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ▪ Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, ▪ Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. ▪ Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: ▪ Dystrybucję certyfikatów poprzez http ▪ Konsolidację CA dla wielu lasów domeny, ▪ Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, ▪ Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869),

	l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 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: ▪ 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) 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. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

	30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

3.2. Zakup zasilaczy awaryjnych UPS Rack - 2 zestawy

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania wraz z informacjami dodatkowymi zgodnie z wymaganiem formularza ofertowego.
Obudowa	Typu Rack, wysokość max 2U, w zestawie szyny montażowe do szafy Rack 19'' Wyposażona w panel sterujący z wyświetlaczem ciekłokrystalicznym LCD oraz sygnalizacją akustyczną wskazujący co najmniej parametry napięcia wejściowego i wyjściowego, częstotliwość oraz pozostałego czasu pracy podczas pracy bateryjnej.
Technologia	VFI-SS-111 zgodnie z PN-EN62040-3 (true on-line, podwójne przetwarzanie energii)
Moc znamionowa	Min. 3 kVA / 3 kW, wyjściowy współczynnik mocy (PF) 1,0
Sprawność AC-AC	1. nie mniejsza niż 93% w trybie pracy on-line z obciążeniem 100% 2. 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.
Sygnały wyjściowe	Napięcie: 230 V Częstotliwość: 50/60Hz (programowalna)
Zintegrowane bezprzerwowe przełączniki obejściowy Bypass	Statyczny przełącznik (SCR) z możliwością ręcznego przełączenia UPSa do trybu Bypass elektroniczny
Czas podtrzymania (wg karty katalogowej producenta)	1. Nie mniej niż 4 minuty przy 100% obciążenia. 2. Nie mniej niż 10 minut przy 50% obciążenia.

Złącze baterii zewnętrznych	Musi istnieć możliwość dołączenia jednostki rozszerzającej wyposażonej w dodatkowe łańcuchy baterii (moduł baterii) wydłużające czas podtrzymania zasilania.
Akumulatory	▪ Szczelne, bezobsługowe, technologia AGM, o projektowanej żywotności min. 10 lat, ▪ Baterie w UPS do wymiany w trybie Hot-Swap 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)
Interfejsy	Złącze interfejsów komunikacyjnych: RS232, USB, slot SNMP 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.
Funkcjonalności dodatkowe	Możliwość regulacji z oprogramowania tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu – wymagana regulacja z Panela LCD
Wyposażenie dodatkowe	Wraz z zasilaczem musi zostać dostarczona karta SNMP do zarządzania UPS z poziomu sieci.
Gwarancja	Min. 2 lata (24 miesiące)

3.3. Zakup zasilaczy awaryjnych UPS do stanowisk komputerowych - 8 zestawów

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania wraz z informacjami dodatkowymi zgodnie z wymaganiem formularza ofertowego.
Moc pozorna	min. 1200VA
Obudowa	Tower wyposażona w graficzny wyświetlacz LCD
Klasa	Line-interactive

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

3.4. Zakup dysków zewnętrznych USB w celu przechowywania odseparowanych od sieci kopii zapasowych – 2 zestawy

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania wraz z informacjami dodatkowymi zgodnie z wymaganiem formularza ofertowego.
Pojemność	5TB
Złącze	USB 3.2
Bezpieczeństwo	256-bitowe szyfrowanie danych AES Ochrona danych za pomocą klucza dostępu
Gwarancja	Min. 2 lata (24 miesiące)

3.5. Zakup licencji dostępowych CAL do środowiska Windows Serwer – 1 pakiet

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania wraz z informacjami dodatkowymi zgodnie z wymaganiem formularza ofertowego.
Zastosowanie	Wymagana jest dostawa pakietu licencji dostępowych CAL RDS do środowiska Windows Serwer pozwalających na uruchomienie usług umożliwiających zapewnienie bezpiecznych połączeń np. w ramach połączeń zdalnych dla użytkownika, który będzie miał możliwość połączenia się bezpośrednio do zasobów serwera z wykorzystaniem logowania domenowego. Zakup licencji ma zapewnić wdrożenie usługi Remote Desktop Services (RDS), gdzie za pomocą

	protokołu Remote Desktop Protocol (RDP) użytkownik uzyska dostęp do pulpitu lub aplikacji instalowanych na serwerze w środowisku Windows Server. Pakiet musi się składać z minimum 6 licencji CAL.

3.6. Zakup licencji do szyfrowania danych - 1 pakiet

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania wraz z informacjami dodatkowymi zgodnie z wymaganiem formularza ofertowego.
Ochrona danych	1. Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022 oraz Microsoft Windows 7/8/10/11. 2. Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2012, 2014, 2016, 2017, 2019 w wersji przynajmniej Express. 3. Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI. 4. Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443. 5. Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish. 6. Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról. 7. Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania. 8. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła. 9. Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej: a) ilość znaków, b) czy hasło ma zawierać wielkie litery,

	c) czy hasło ma zawierać małe litery, d) czy hasło ma zawierać cyfry, e) czy hasło ma zawierać znaki specjalne, f) okres ważności, g) ilość nieudanych logowań. 10. Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych. 11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej: a) ilość znaków, b) czy hasło ma zawierać wielkie litery, c) czy hasło ma zawierać małe litery, d) czy hasło ma zawierać cyfry, e) czy hasło ma zawierać znaki specjalne, f) fokres ważności, g) ilość nieudanych logowań, h) możliwość zmiany hasła. 12. Konsola centralnego zarządzania musi gromadzić informacje o: a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych, b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych, c) dacie aktywacji klienta systemu szyfrowania danych, d) statusu szyfrowania, e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych, f) stanie polityki, g) wersji klienta systemu szyfrowania danych, h) wersji systemu operacyjnego stacji roboczej, i) użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej. 13. Konsola musi być dostępna z poziomu interfejsu WWW.

	14. Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet. 15. Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych. 16. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny: a) instalacji klienta na stacji, b) zaszyfrowania/odszyfrowania stacji, c) wygenerowania klucza aktywacyjnego dla użytkownika, d) administrowania kluczami szyfrującymi, e) administrowania użytkownikami, którzy mają dostęp do stacji, f) administrowania profilem ustawień dla użytkowników, g) administrowania profilem ustawień dla stacji roboczych, h) wymuszenia zmiany hasła, i) zarządzania wieloma organizacjami z poziomu jednej konsoli
Wymagania systemowe aplikacja klienckiej	System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10/11 oraz w środowiskach Microsoft Windows Server 2012, 2012 R2, 2016, 2019, 2022.
Wymagania dotyczące uwierzytelniania	1. Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file). 2. Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows.
Wymagania dotyczące ustawień aplikacji klienckiej	1. Wymagany interfejs w języku polskim i angielskim. 2. Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób: a) sektor po sektorze, b) kontener. 3. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła. 4. Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami.

	5. Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail. 6. Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego. 7. Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania. 8. Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania. 9. Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania. 10. Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego. 11. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego. 12. Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła. 13. Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB. 14. Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła. 15. Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów: a) Guttman. b) US Department of Defence 5220.22-M (8-306. /E). c) US Department of Defence 5220.22-M (8-306. /E, CiE). d) Kryptograficzne losowe dane liczbowe. 16. Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.

	17. Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego. 18. Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie. 19. Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji. 20. Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI.
Wymagania dotyczące szyfrowania	Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania: 1. AES (Rijndael). 2. Blowfish. 3. cTriple DES (3DES).
Liczba licencji	Wymagane jest dostarczenie pakietu licencji bezterminowej dla 20 stanowisk wraz ze wsparciem w okresie realizacji projektu, tj. do dnia. 30.06.2026

3.7. Zakup zarządzalnych przełączników sieciowych - 2 zestawy

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania wraz z informacjami dodatkowymi zgodnie z wymaganiem formularza ofertowego.
Funkcjonalność	Wymagane protokoły routingu warstwy 3 wspierające skalowanie sieci, statyczny routing, RIP, OSPF, ECMP, VRRP, Serwer DHCP i DHCP Relay.
Strategie bezpieczeństwa	ACL, Ochrona portów, Ochrona przed atakami DoS, 802.1X
Funkcje bezpieczeństwa	Funkcje zapewniające ochronę sieci przed wieloma zagrożeniami ACL (IPv4 i IPv6), dynamiczna inspekcja ARP, IEEE 802.1X, MAB, ochrona portów i Secure Shell (SSH).
Obudowa	Przełącznik musi być w formacie umożliwiającym jego montaż w standardowej szafie Rack 19” oraz musi posiadać w zestawie odpowiednie uchwyty montażowe.
Porty	Porty 1GbE - 48 gigabitowych portów Base-T PoE+:

	Porty 10GbE - 4 porty SFP+ Port konsolowy Port zarządzający
Standardy PoE	Standardy: 802.3at/af
Sieci VLAN	Obsługa 4K identyfikatorów VLAN Funkcja umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) Tagowanie 802.1Q VLAN, Multicast VLAN, VLAN zarządzania, VLAN VPN (QinQ), GVRP, VLAN VPN, Głosowa sieć VLAN, Prywatny VLAN
Wydajność	Rozmiar tablicy adresów MAC urządzenia min. 30K Min. przepustowość urządzenia 160 Gbps
Gwarancja	Min. 2 lata (24 miesiące)

3.8. Zakup licencji oprogramowania antywirusowego z aktywną ochroną w okresie realizacji projektu - 1 pakiet

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania wraz z informacjami dodatkowymi zgodnie z wymaganiem formularza ofertowego.
Ochrona stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

	7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

	b) tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, c) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, d) tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, e) tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: a) tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

	b) tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, c) tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, d) tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum
Ochrona serwerów	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

	4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

	15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
Administracja zdalna w chmurze	1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.

	7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
Szyfrowanie	1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i Microsoft Windows 11 64-bit. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android	1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a) usunięcie zawartości urządzenia, b) przywrócenie urządzenie do ustawień fabrycznych, c) zablokowania urządzenia, d) uruchomienie sygnału dźwiękowego, e) lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a) nazwę aplikacji, b) nazwę pakietu, c) kategorię sklepu Google Play, d) uprawnienia aplikacji, e) pochodzenie aplikacji z nieznanego źródła.
Sandbox w chmurze	1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.

	6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: a) Czysty, b) Podejrzany, c) Bardzo podejrzany, d) Szkodliwy. 13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia
Moduł XDR	1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

	2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

	13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 16. Konsola administracyjna musi mieć możliwość tagowania obiektów. 17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
Liczba licencji	Wymagane jest dostarczenie pakietu licencji dla 30 stanowisk wraz z aktywną ochroną (tj. wsparciem technicznym oraz subskrypcją), zapewnioną w okresie realizacji projektu na okres 24 miesięcy, lecz nie dłużej niż do 30.06.2026 r.

3.9. Zakup licencji oprogramowania do realizacji kopii zapasowych - 1 pakiet

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego rozwiązania wraz z informacjami dodatkowymi zgodnie z wymaganiem formularza ofertowego.
Wymagania ogólne	1. 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. 2. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Całkowite koszty posiadania	1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. 2. Oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków. 3. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji 4. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. 5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. 6. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. 7. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. 8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania

	9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) 10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu 11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API 12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji 13. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji 14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania 15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. 16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej 17. Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora) 18. Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS) 19. Oprogramowanie musi posiadać integracje z systemami typu SIEM. 20. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
Wymagania RPO	1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej

	2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru 4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. 5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. 6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (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. 11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V.

	Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. 12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. 13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik 14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding). 15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Wymagania RTO	1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. 2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) 3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami 4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre 5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, 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.

	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 lokalizacji 20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN 21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle 22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI 23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2. 24. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Ograniczenie ryzyka	1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) 2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. 3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego

	harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem 4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. 5. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware 6. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania 7. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków 8. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Środowiska fizyczne	1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego 2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych 3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE 4. Rozwiązanie musi wspierać system operacyjny macOS 5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix

	6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) 7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster 8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów 9. Rozwiązanie musi wspierać backup podłączonych dysków USB 10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym 11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) 12. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone 13. Rozwiązanie musi wspierać kontrolę pasma sieciowego 14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych 15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN 16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft 17. Rozwiązanie musi wspierać technologię BitLocker 18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania 19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint

	2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych 20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych 21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, 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 24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne 25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego 26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej. 27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
Monitoring	1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich 2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie 3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server

	zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. 4. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter 5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn 6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel 7. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk 8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora 9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów 10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) 11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna 12. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego 13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta 14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. 15. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania

	jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. 16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware 17. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4
Raportowanie	1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie 2. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. 3. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. 4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V 5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF 6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc 7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach 8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów 9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych

	10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych 11. System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury 12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta 13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. 14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'. 15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware 16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) 17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie
Liczba licencji	1. Wymagane jest dostarczenie licencji bezterminowej wraz z aktywną ochroną (wsparciem technicznym), zapewnioną w okresie realizacji projektu na okres 24 miesięcy, lecz nie dłużej niż do 30.06.2026 r. 2. Licencja musi zapewnić realizację kopii zapasowych z serwera fizycznego oraz 4 maszyn wirtualnych (VM).

3.10. Utrzymanie wsparcia technicznego wraz z subskrypcjami dla posiadanego oprogramowania do realizacji kopii zapasowych - 1 pakiet

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie nazwy serwisów i licencji oraz okresu oferowanego wsparcia.

Rodzaj wsparcia	W celu zapewnienia aktualnego wsparcia, Zamawiający wymaga dostarczenia aktualizacji wsparcia technicznego wraz z subskrypcjami dla posiadanej licencji do realizacji kopii zapasowych pod nazwą „Veeam Backup Essentials Universal Perpetual License. Includes Enterprise Plus Edition features." Licencje oraz serwisy powinny mieć zapewnione wsparcie techniczne oraz subskrypcję na okres 24 miesięcy, w okresie realizacji projektu, lecz nie dłużej niż do 30.06.2026 r. Zamawiający informuję, że posiada 1 licencję przewidzianą dla 5 instancji (5 wystąpień).

3.11. Utrzymanie wsparcia technicznego wraz z subskrypcjami dla posiadanego UTM - 1 pakiet

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie nazwy serwisów i licencji oraz okresu oferowanego wsparcia.
Rodzaj wsparcia	W celu zapewnienia aktualnej ochrony sieci wewnętrznej, Zamawiający wymaga dostarczenia pakietów licencji oraz serwisów (subskrypcji) dla posiadanego urządzenia UTM Stormshield SN310. Zamawiający wymaga dostarczenia licencji dla wszystkich funkcji bezpieczeństwa, które posiada w ramach zakupionej licencji, tj. 1. Opcję serwisową UTM Security Pack (FW+IPS, VPN, filtr URL, AV, AS, Obsługa kart SD). 2. Wznowienie gwarancji na dostarczone elementy systemu w formule NBD tzn. w przypadku awarii urządzenia nastąpi wymiana urządzenia na sprawne (lub na urządzenie zastępcze) najpóźniej w kolejny dzień roboczy od potwierdzenia awarii. W ramach niniejszego projektu powyższe licencje oraz serwisy powinny zostać wznowione na okres 24 miesięcy, w okresie realizacji projektu, lecz nie dłużej niż do 30.06.2026 r.

3.12. Utrzymanie wsparcia technicznego wraz z subskrypcjami dla posiadanego oprogramowania do zarządzania zasobami IT - 1 pakiet

KRYTERIUM	WYMAGANE MINIMALNE PARAMETRY
Typ	W ofercie wymagane jest podanie nazwy serwisów i licencji oraz okresu oferowanego wsparcia.
Rodzaj wsparcia	W celu zapewnienia aktualnego wsparcia, Zamawiający wymaga dostarczenia aktualizacji wsparcia technicznego wraz z subskrypcjami dla posiadanej licencji oprogramowania od zarządzania zasobami i procesami IT pod nazwą „IT Manager" firmy Infonet Projekt S.A. Licencje oraz serwisy powinny mieć zapewnione wsparcie techniczne (polisę serwisową) gwarantującą świadczenie usługi supportu przez okres 24 miesięcy, w okresie realizacji projektu, lecz nie dłużej niż do 30.06.2026 r. w wariancie Support Premium wraz z dostęp do nowych wersji systemu w ramach posiadanych modułów systemu ITManager. Zamawiający informuje, że wymaga dostawy suportu dla pakietu obejmującego moduły: 1. Moduły ITM AGENT WINDOWS: a) Baza konfiguracji komputerów oraz oprogramowania b) Zarządzanie zasobami oraz użytkownikami (100) c) Zarządzanie licencjami, audyt oprogramowania d) Monitoring plików e) Zdalny pulpit, zdalne zarządzanie komputerem f) Automatyzacja (Zarządzanie Zadaniami, Zarządzanie Polisami, Grupy Dynamiczne, Makra) g) Zarządzanie urządzeniami USB storage h) Backup Danych Użytkownika i) Monitoring użytkowników (Aplikacje, Strony WWW, Wydruki) 2. Moduły DODATKOWE: a) ServiceDesk (Server: Lite; ilość UserCal: 30) b) Opcja Zarządzanie Wnioskami c) Opcja Zarządzanie Uprawnieniami d) Skaner Sieci (Server: Lite; ilość DeviceCal: 100)