Opis Przedmiotu Zamówienia

na dostawę, konfigurację oraz wdrożenie sprzętu i oprogramowania

związanych z realizacją projektu

„Cyberbezpieczny Samorząd”

dla Powiatu Łosickiego

Opis Przedmiotu Zamówienia

Cyberbezpieczny Samorząd — Powiat Łosicki

Dokument stanowi opis przedmiotu zamówienia dla postępowania realizowanego w ramach projektu „Cyberbezpieczny Samorząd” dla Powiatu Łosickiego.

Nazwy pozycji (kategorii) zamówienia przyjęto zgodnie z nazewnictwem Zamawiającego. Wymagania funkcjonalne, techniczne i parametry minimalne określono w częściach szczegółowych niniejszego dokumentu.

Część ogólna — zasada równoważności i neutralności technologicznej

Zasada równoważności rozwiązań i neutralności technologicznej.

- Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.

- Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.

- Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.

- Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.

- Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.

- W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.

- Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.

- Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

- W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

- W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza

prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

- Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

- Za równoważną do normy ISO 9001 Zamawiający uzna normę, która dotyczy zarządzania jakością ustanawiając wymagania dla systemów zarządzania jakością w organizacjach w minimum następującym zakresie:

    a. Skupienie na użytkowniku – Podstawowym celem systemu zarządzania jakością jest zwiększenie satysfakcji użytkownika poprzez spełnianie jego wymagania oraz oczekiwania. Organizacja powinna monitorować potrzeby użytkowników i dostarczać produkty lub usługi, które je zaspokajają.

    b. Przywództwo – Wspieranie kierownictwa w zapewnianiu odpowiednich zasobów i wsparcia w procesach zarządzania jakością. Przywódcy powinni tworzyć środowisko, które wspiera zaangażowanie pracowników w poprawę jakości.

    c. Zaangażowanie ludzi – Organizacja powinna zapewnić, aby wszyscy pracownicy byli zaangażowani w realizację celów jakościowych. Kluczowym elementem jest angażowanie personelu w procesy poprawy jakości i podejmowanie działań na rzecz doskonalenia.

d. Podejście procesowe – Norma podkreśla, że organizacja powinna zarządzać swoimi procesami w sposób spójny i skuteczny, traktując je jako powiązane ze sobą elementy systemu zarządzania jakością, które wspólnie prowadzą do osiągania celów organizacji.

e. Podejście systemowe do zarządzania – Organizacja powinna traktować system zarządzania jakością jako całość, złożoną z wzajemnie powiązanych elementów (np. procesów, zasobów, technologii), które muszą działać w harmonii, aby osiągnąć cele jakościowe.

f. Ciągłe doskonalenie – dążenie do ciągłego doskonalenia procesów w organizacji. Ciągłe doskonalenie jest kluczowym elementem skutecznego zarządzania jakością i poprawy wyników.

g. Podejście do podejmowania decyzji oparte na faktach – w procesie podejmowania decyzji organizacja powinna opierać się na danych i analizach, a nie na przypuszczeniach czy intuicji. Podejście to pozwala na bardziej precyzyjne i obiektywne decyzje.

h. Relacje z dostawcami na zasadzie wzajemnych korzyści – tworzenie partnerskich relacji z dostawcami, które będą korzystne dla obu stron. Współpraca z dostawcami powinna być oparta na zaufaniu i dążeniu do wspólnych celów jakościowych.

i. Zarządzanie ryzykiem – norma wymaga, aby organizacje identyfikowały, oceniały i zarządzały ryzykiem związanym z procesami oraz ich wpływem na zdolność organizacji do dostarczania produktów i usług o wymaganej jakości.

j. Dokumentowanie systemu zarządzania jakością – Norma określa wymagania dotyczące dokumentowania systemu zarządzania jakością, w tym tworzenia polityki jakości, procedur, instrukcji roboczych oraz zapisów, które umożliwiają monitorowanie i weryfikację skuteczności systemu.

- Za równoważną do normy ISO 50001 Zamawiający uzna normę, która dotyczy zarządzania energią w organizacjach w minimum następującym zakresie:

a. Skupienie na poprawie efektywności energetycznej – Celem normy jest poprawa efektywności wykorzystania energii poprzez identyfikację obszarów, w których możliwe są oszczędności i usprawnienia w zarządzaniu energią.

b. Zarządzanie cyklem życia energii – uwzględnia cały cykl życia energii, od planowania, poprzez wykorzystanie, aż po monitorowanie, ocenę i doskonalenie działań mających na celu zmniejszenie zużycia energii.

c. Zintegrowane podejście z innymi systemami zarządzania – Norma jest zaprojektowana w sposób zgodny z innymi międzynarodowymi normami, co umożliwia integrację systemów zarządzania w organizacji.

d. Podejście oparte na cyklu PDCA (Plan-Do-Check-Act) – opiera się na cyklu PDCA, który wspiera organizacje w procesie ciągłego doskonalenia zarządzania energią poprzez planowanie, wdrażanie, monitorowanie i działania korygujące.

e. Zaangażowanie kierownictwa – Norma wymaga, aby najwyższe kierownictwo organizacji angażowało się w proces zarządzania energią, podejmując decyzje, dostarczając zasoby oraz ustalając cele i polityki energetyczne.

f. Ustalenie polityki energetycznej – norma zachęca organizacje do opracowania polityki energetycznej, która definiuje kierunki działań, cele efektywności energetycznej oraz zobowiązania do ciągłego doskonalenia.

g. Identyfikacja i ocena aspektów energetycznych – Norma wymaga przeprowadzenia analizy aspektów energetycznych, które mają istotny wpływ na zużycie energii i środowisko, oraz wdrożenia działań na rzecz ich poprawy.

h. Monitorowanie, pomiar i analiza – nakłada obowiązek monitorowania i mierzenia zużycia energii oraz wydajności energetycznej organizacji. Organizacja powinna także stosować odpowiednie narzędzia do analizy wyników, identyfikacji możliwości poprawy oraz podejmowania działań korygujących.

i. Zarządzanie ryzykiem i szansami – Norma podkreśla znaczenie identyfikacji ryzyk i szans związanych z zarządzaniem energią, a także działań na rzecz minimalizowania ryzyka i maksymalizowania możliwości poprawy efektywności energetycznej.

j. Ciężar działań edukacyjnych i szkoleń – Norma wskazuje na konieczność zapewnienia odpowiedniego poziomu wiedzy i umiejętności w zakresie zarządzania energią dla wszystkich pracowników organizacji. Szkolenia i podnoszenie świadomości energetycznej są kluczowe dla skutecznego wdrażania polityki energetycznej.

- Za równoważną do normy ISO 14001 Zamawiający uzna normę, która dotyczy systemów zarządzania środowiskowego w minimum następującym zakresie:

a. Zarządzanie środowiskowe oparte na cyklu PDCA (Plan-Do-Check-Act) – norma opiera się na cyklu PDCA, który wspiera organizacje w systematycznym zarządzaniu i doskonaleniu ich działań na rzecz ochrony środowiska. Proces obejmuje planowanie, wdrażanie, monitorowanie oraz podejmowanie działań korygujących.

b. Zobowiązanie organizacji do ochrony środowiska – Norma wymaga, aby organizacja była zobowiązana do minimalizowania negatywnego wpływu na środowisko. To zobowiązanie powinno być wyrażone poprzez politykę środowiskową, która wskazuje na cele ochrony środowiska.

c. Identyfikacja aspektów środowiskowych – Organizacja musi identyfikować i oceniać aspekty środowiskowe związane z jej działalnością, produktami i usługami. Ocena powinna uwzględniać wpływ na środowisko, zarówno w zakresie zużycia zasobów, jak i wytwarzania odpadów oraz emisji.

d. Zgodność z przepisami prawnymi i innymi wymaganiami – norma wymaga, aby organizacja przestrzegała obowiązujących przepisów prawnych dotyczących ochrony środowiska oraz innych zobowiązań, które organizacja uzna za stosowne (np. normy branżowe).

e. Cele środowiskowe i planowanie działań – Organizacja musi wyznaczać mierzalne cele środowiskowe i opracować plany działań, które pozwolą osiągnąć te cele. Cele te powinny być zgodne z polityką środowiskową i uwzględniać aspekt środowiskowy w całym cyklu życia produktów i usług.

f. Zaangażowanie kierownictwa – zaangażowanie najwyższego kierownictwa w wdrażanie systemu zarządzania środowiskowego. Kierownictwo powinno zapewnić zasoby, nadzór i wspierać działania na rzecz ochrony środowiska.

g. Zarządzanie ryzykiem środowiskowym – Norma podkreśla konieczność identyfikacji i oceny ryzyk środowiskowych związanych z działalnością organizacji. Organizacja powinna podejmować działania na rzecz minimalizowania ryzyk, a także wdrażać procedury zapobiegania i reagowania na sytuacje kryzysowe.

h. Monitorowanie, pomiar i analiza wyników – Organizacja jest zobowiązana do monitorowania i mierzenia skuteczności swoich działań środowiskowych. Obejmuje to ocenę wpływu działań na środowisko, skuteczność realizacji celów oraz identyfikację obszarów do poprawy.

i. Działania korygujące i zapobiegawcze – norma wymaga, aby organizacja wdrażała procedury podejmowania działań korygujących w przypadku niezgodności oraz działań zapobiegawczych, aby uniknąć powtarzania się problemów środowiskowych w przyszłości.

j. Ciągłe doskonalenie systemu zarządzania środowiskowego – Podstawowym celem normy jest dążenie do ciągłego doskonalenia systemu zarządzania środowiskowego. Organizacja powinna regularnie przeglądać i aktualizować swoje cele, polityki i procesy, aby dostosować je do zmieniających się warunków środowiskowych oraz wymagań prawnych.

- Za równoważną do normy ISO 27001 Zamawiający uzna normę, która określa standard zarządzania bezpieczeństwem informacji w minimum następującym zakresie:

a. Zarządzanie ryzykiem – norma stosuje podejście oparte na zarządzaniu ryzykiem. Organizacja musi przeprowadzać ocenę ryzyka dla bezpieczeństwa informacji i podejmować odpowiednie środki w celu zarządzania tym ryzykiem.

b. Ochrona informacji – Norma zapewnia, że organizacja identyfikuje, ocenia i zabezpiecza informacje, w tym dane osobowe, finansowe, techniczne, i inne zasoby przed zagrożeniami.

c. Ciągłość działania – norma kładzie nacisk na ciągłość działania w przypadku awarii systemów, katastrof naturalnych, ataków cybernetycznych itp. Organizacje muszą przygotować plany awaryjne i procedury odzyskiwania danych.

d. Zaangażowanie kierownictwa – Norma wymaga aktywnego zaangażowania najwyższego kierownictwa w procesie zarządzania bezpieczeństwem informacji.

e. Ciągłe doskonalenie –norma promuje ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji, aby dostosować go do zmieniających się zagrożeń i wymagań.

f. Polityki bezpieczeństwa informacji – norma określa, że organizacja musi opracować i wdrożyć formalne polityki bezpieczeństwa informacji, które są zgodne z jej celami biznesowymi i wymaganiami regulacyjnymi.

g. Szkolenia i świadomość pracowników – norma kładzie nacisk na edukację i szkolenia pracowników w zakresie bezpieczeństwa informacji. Wszyscy pracownicy muszą być świadomi swoich obowiązków w zakresie ochrony danych.

h. Zarządzanie dostępem – norma wymaga, aby dostęp do informacji i zasobów organizacji był kontrolowany i ograniczony na podstawie ról i odpowiedzialności pracowników.

i. Monitorowanie i przeglądy – norma określa, że organizacje muszą regularnie monitorować skuteczność wdrożonego systemu zarządzania bezpieczeństwem informacji oraz przeprowadzać audyty, które pozwolą ocenić zgodność z wymaganiami normy.

j. Zgodność z przepisami prawa – norma wymaga, aby organizacje zapewniały zgodność z obowiązującymi przepisami prawnymi dotyczącymi ochrony danych osobowych, ochrony prywatności i bezpieczeństwa informacji.

- Za równoważną do regulacji RoHS Zamawiający uzna regulację, która dotyczy stosowania substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym w minimum następującym zakresie:

a. Zakaz stosowania niebezpiecznych substancji – ogranicza użycie sześciu substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym: ołów (Pb), rtęć (Hg), kadm (Cd), sześciowartościowy chrom (Cr^6), polibromowane bifenyly (PBB) i polibromowane etery difenylowe (PBDE).

b. Zastosowanie do sprzętu elektronicznego i elektrycznego – obejmuje szeroki zakres produktów, takich jak telewizory, komputery, sprzęt AGD, zabawki, oświetlenie LED, urządzenia medyczne, sprzęt telekomunikacyjny i inne urządzenia elektroniczne.

c. Zobowiązanie producentów do zgodności – Producenci i importerzy sprzętu elektrycznego i elektronicznego muszą zapewnić, że ich produkty nie zawierają zabronionych substancji powyżej dopuszczalnych poziomów.

d. Oświadczenia o zgodności – Producenci są zobowiązani do dostarczania odpowiednich oświadczeń o zgodności z regulacją. Powinny one być udostępniane organom nadzoru oraz użytkownikom w razie potrzeby.

e. Kontrola i nadzór rynkowy – regulacja nakłada obowiązek przeprowadzania kontroli rynkowych przez odpowiednie organy państwowe, aby upewnić się, że produkty wprowadzane na rynek UE spełniają wymogi dyrektywy.

f. Ograniczenie wpływu na zdrowie i środowisko – celem regulacji jest zmniejszenie negatywnego wpływu niebezpiecznych substancji na zdrowie ludzi oraz na środowisko naturalne, szczególnie podczas recyklingu i utylizacji odpadów elektronicznych.

g. Zdolność do recyklingu i odzysku – regulacja promuje projektowanie produktów w sposób, który umożliwia ich łatwiejszy recykling i utylizację. Przepisy zakładają, że zabronione substancje nie mogą występować w produktach w ilościach, które utrudniają ich odzyskiwanie.

h. Zakres geograficzny – regulacja ma zastosowanie w krajach Unii Europejskiej oraz w krajach, które przyjęły odpowiednie przepisy zgodne z dyrektywą.

i. Obowiązki w przypadku modyfikacji produktów – W przypadku wprowadzenia istotnych zmian w produkcie (np. zmiana jego konstrukcji), producent musi upewnić się, że nowa wersja również spełnia wymagania regulacji. Dotyczy to również produktów wprowadzanych na rynek wtórny (np. w ramach naprawy lub refabrykacji).

- Za równoważną do regulacji CE Zamawiający uzna regulację, która spełnia wszystkie odpowiednie wymagania dotyczące zdrowia, bezpieczeństwa oraz ochrony środowiska, zgodnie z przepisami UE w minimum następującym zakresie:

  a. Potwierdzenie zgodności z wymaganiami UE – formalne oświadczenie producenta lub importera, że dany produkt spełnia wszystkie obowiązujące przepisy unijne dotyczące zdrowia, bezpieczeństwa, ochrony środowiska i innych przepisów regulujących dany produkt.

  b. Oznakowanie CE – posiada system oznaczeń, który wskazuje, że produkt przeszedł ocenę zgodności i jest dopuszczony do sprzedaży w Unii Europejskiej.

  c. Szczegółowe informacje o producencie – dokument potwierdzający musi zawierać pełne dane producenta (lub importera), takie jak nazwa firmy, adres siedziby, a także dane kontaktowe. W przypadku importera – także informacje o tym, kto odpowiada za dany produkt w UE.

  d. Opis produktu – dokument potwierdzający musi zawierać szczegółowy opis produktu, który obejmuje nazwę produktu, numer referencyjny lub numer katalogowy, a także inne identyfikatory, które umożliwiają jednoznaczną identyfikację produktu.

  e. Odniesienia do odpowiednich norm – dokument potwierdzający wskazuje normy, dyrektywy lub przepisy unijne, z którymi produkt jest zgodny.

  f. Procedura oceny zgodności – dokument potwierdzający musi wskazywać, w jaki sposób ocena zgodności produktu została przeprowadzona (np. przez samodzielną ocenę producenta lub poprzez współpracę z jednostką notyfikowaną w przypadku bardziej skomplikowanych produktów).

  g. Data i miejsce sporządzenia deklaracji – dokument potwierdzający powinien zawierać datę sporządzenia deklaracji oraz miejsce jej podpisania, co ma znaczenie prawne i daje pewność co do okresu ważności oświadczenia.

h. Podpis osoby upoważnionej – dokument potwierdzający musi być podpisana przez osobę upoważnioną w imieniu producenta lub importera, która jest odpowiedzialna za prawdziwość oświadczenia. Zwykle jest to przedstawiciel firmy, który ma uprawnienia do składania oświadczeń w imieniu organizacji.

i. Wymóg dostępności dla organów nadzoru – dokument potwierdzający musi być dostępny dla odpowiednich organów nadzoru rynkowego, które mogą przeprowadzać kontrole w celu weryfikacji zgodności produktów z obowiązującymi wymaganiami.

j. Zakres odpowiedzialności producenta – dokument potwierdzający musi być dokumentem, który wiąże producenta z odpowiedzialnością za zgodność produktu z wymaganiami prawnymi i normatywnymi. Jeżeli produkt nie spełnia wymagań, producent lub importer mogą być pociągnięci do odpowiedzialności za naruszenie przepisów UE.

- Za równoważną do certyfikacji FIPS 140-2 Zamawiający uzna certyfikację, która dotyczy standardu wymagań bezpieczeństwa dla modułów kryptograficznych w minimum następującym zakresie:

  a. Obejmuje wszystkie komponenty sprzętowe, oprogramowanie i kombinacje tych elementów, które realizują operacje kryptograficzne (np. szyfrowanie, podpisy cyfrowe, generowanie kluczy).

  b. Wymaga, aby moduły kryptograficzne posiadały odpowiednią ochronę przed manipulacjami fizycznymi.

  c. Wymaga, aby wszystkie klucze kryptograficzne były odpowiednio chronione. Obejmuje to m.in. przechowywanie, generowanie, zarządzanie i wymianę kluczy w sposób, który zapobiega ich nieautoryzowanemu ujawnieniu.

  d. Nakłada wymagania dotyczące bezpiecznego uruchamiania modułu kryptograficznego, w tym procedury inicjalizacji, które muszą zapewniać, że urządzenie jest w pełni zabezpieczone przed uruchomieniem jakichkolwiek operacji kryptograficznych.

  e. Wymaga, aby systemy kryptograficzne były testowane pod kątem zabezpieczeń kryptograficznych.

  f. Definiuje wymagania dotyczące implementacji standardowych algorytmów kryptograficznych.

  g. Wymaga, aby systemy kryptograficzne były odpowiednio utrzymywane przez cały okres ich użytkowania.

Część I. Licencje i oprogramowanie IT z zakresu cyberbezpieczeństwa

Lp.	Nazwa pozycji	Ilość / zakres	Kody CPV
1.	Oprogramowanie do zarządzania infrastrukturą IT	1 instancja (ITSM/CMDB) oraz 60 stacji roboczych (zarządzanie końcówkami i inwentaryzacja)	48000000-8; 48731000-4

2.	Oprogramowanie do kopii zapasowych	1 instancja wraz z licencjami dla wskazanych serwerów, VM i zasobów	48614000-5; 48000000-8; 48731000-4
3.	Oprogramowanie DLP wraz ze wsparciem — pakiet 50 licencji	55 stacji roboczych	48731000-4; 48000000-8
4.	System do zbierania i analizy logów	1 instancja	48731000-4; 48219100-7; 48000000-8
5.	Oprogramowanie do zarządzania podatnościami — pakiet 50 licencji	1 instancja	48731000-4; 48000000-8
6.	Oprogramowanie wspomagające zarządzanie ryzykiem, zgłaszanie incydentów i audyty	1 instancja	48731000-4; 48000000-8

Ogólne wymagania wspólne dla zamówienia

- Rozwiązania muszą być przeznaczone do eksploatacji w środowisku jednostki samorządu terytorialnego,
  z uwzględnieniem ochrony danych osobowych, ciągłości działania, rozliczalności działań administratorów oraz bezpieczeństwa infrastruktury IT.

- Wykonawca musi zapewnić, że oferowane licencje obejmują wszystkie funkcje wymagane w OPZ; niedopuszczalne jest zaoferowanie rozwiązania, które wymaga zakupu dodatkowych modułów dla spełnienia wymagań minimalnych.

- Rozwiązania muszą umożliwiać bezpieczne uwierzytelnianie administratorów i operatorów, nadawanie uprawnień według ról oraz rejestrowanie czynności administracyjnych w zakresie właściwym dla danego systemu.

- Tam, gdzie system przetwarza dane Zamawiającego, musi zapewniać możliwość eksportu danych lub raportów w powszechnie stosowanych formatach, w szczególności PDF, CSV, XLSX lub równoważnych.

- Wdrożenie nie może naruszać działania istniejących usług produkcyjnych Zamawiającego; prace konfiguracyjne wymagające przerw muszą być uzgodnione z Zamawiającym.

- Wykonawca musi przekazać Zamawiającemu dokumentację powdrożeniową umożliwiającą samodzielną eksploatację rozwiązania po zakończeniu wdrożenia.

- Wykonawca musi zapewnić instruktaż administratorów obejmujący podstawową administrację, obsługę incydentów/alertów, raportowanie, aktualizacje, wykonywanie kopii konfiguracji oraz procedury odtworzeniowe, o ile dotyczą danej pozycji.

Poz. 1. Oprogramowanie do zarządzania infrastrukturą IT

Pozycja obejmuje dwa komplementarne zakresy funkcjonalne opisane poniżej: zarządzanie usługami IT (ITSM/CMDB) oraz zarządzanie końcówkami i inwentaryzację IT.

Zakres A — zarządzanie usługami IT (ITSM/CMDB)

Ilość: 1 instancja (2 administratorów)

CMDB

- Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI)
- Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe
- Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI
- Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny
- Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI
- Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji
- Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej
- Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji
- Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami
- Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji
- Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV)
- Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji
- Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów
- Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej
- Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji

Zarządzanie zasobami oraz użytkownikami

- Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.

- Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
- Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
- Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
- Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1: N wraz z podglądem przypisanych zasobów oraz wydrukiem.
- Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
- Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.
- Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu.
- Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
- Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
- Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu
- Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF
- Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków
- Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji
- Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu
- Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu
- Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu
- Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu
- Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego
- Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu
- Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami

- Oprogramowanie musi umożliwiać seryjne dodawanie zasobów
- Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów
- Oprogramowanie musi udostępniać kreator raportów dla zasobów
- Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu
- Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu
- Oprogramowanie musi umożliwiać ewidencję magazynów
- Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych
- Oprogramowanie musi umożliwiać ewidencję produktów magazynowych
- Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo)
- Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM
- Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn
- Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu
- Oprogramowanie musi umożliwiać zwrot zasobów na magazyn
- Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM
- Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie
- Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca)
- Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji
- Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników
- Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji
- Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników
- Oprogramowanie musi umożliwiać zarzadzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami

  Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS

ServiceDesk – Zarządzanie zgłoszeniami

Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:

- Zarządzanie problemem
- Zarządzanie incydentem

- Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
- Zarządzanie umowami serwisowymi
- Definicje poziomów SLA (reakcja, naprawa, reklamacja)
- Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.
- Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.
- Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
- Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
- Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
- Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
- Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
- Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
- Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
- Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
- Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
- Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.
- Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.
- Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
- Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
- Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
- Oprogramowanie musi umożliwiać tworzenie szablonów zadań.

- Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.
- Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
- Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.
- Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
- Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.
- Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.
- Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.
- Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.
- Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.
- Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera).
- Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).
- Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.
- Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
- Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.
- Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.
- Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
- Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.

- Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji
- mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
- Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).
- Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
- Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.
- Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)

Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:

- Zmiana statusu po przejęciu zgłoszenia przez opiekuna.
- Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna.
- Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia.
- Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika.
- Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika.
- Zamykanie zgłoszenia po upływie czasu reklamacji.
- Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów.
- Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.
- Walidacja zamkniętych zadań w zamykanym zgłoszeniu.
- Systemowe potwierdzanie realizacji zgłoszenia.
- Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.
- Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.

- Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.
- Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.
- Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).
- Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika
- Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia
- Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń)
- Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem
- Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB
- Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)
- Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia
- Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia
- Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)
- Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu
- Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą
- Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności
- Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu
- Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.
- Oprogramowanie musi umożliwiać definiowanie obiegów za pomocą graficznego/blokowego kreatora.
- Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.
- Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.

- Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.
- Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.
- Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.
- Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.
- Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.
- Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.
- Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.
- Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.
- Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.

ServiceDesk – Zarządzanie wnioskami

- Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).
- Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.
- Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.

ServiceDesk – Zarządzanie uprawnieniami

- Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych
- Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych
- Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)
- Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
- Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek

- Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
- Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
- Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
- Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
- Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
- Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
- Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika

ServiceDesk – Zarządzanie rezerwacjami

- Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
- Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
- Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.
- Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.
- Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.
- Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

Zarządzanie dokumentami

- Oprogramowanie musi umożliwiać centralną ewidencję dokumentów
- Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu
- Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów)
- Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów
- Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników
- Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym
- Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących
- Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany.

Zakres B — zarządzanie końcówkami i inwentaryzacja IT

Ilość: licencja na 60 stacji roboczych, 2 administratorów

Wymagania ogólne dla systemu zarządzania procesami, usługami i końcówkami

- Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
- Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
- Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
- Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
- Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.
- Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
- Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.
- Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
- Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
- Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
- Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
- Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
- Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych.
- Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.

- Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).
- Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
- Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
- Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
- Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
- Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
- Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
- Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
- Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
- Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
- Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
- Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
- Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).
- Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.

- Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
- Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
- Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

Inwentaryzacja konfiguracji komputerów

- Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
- Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
- Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
- Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
- Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
- Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.

Oprogramowanie musi umożliwiać analizę sprzętową:

- płyty głównej w zakresie model, producent, nr. seryjny,
- CPU w zakresie nazwy, modelu, producenta, częstotliwości,
- HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
- RAM w zakresie wielkości pamięci,
- karty sieciowej w zakresie model, adres IP, adres MAC,
- karty graficznej w zakresie model.

- Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
- Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
- Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.

- Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
- Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
- Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
- Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)
- Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB
- Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)
- Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

Inwentaryzacja oprogramowania

- Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
- Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
- Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
- Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
- Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
- Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
- Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
- Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
- Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.

- Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

Zarządzanie licencjami, audyt oprogramowania

- Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
- Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych
  w procesie automatycznego audytu licencji (rozliczenie ilościowe).
- Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
- Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
- Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

Zdalny pulpit, zdalne zarządzanie komputerem

- Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
- Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
- Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
- Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
- Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
- Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
- Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
- Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.

- Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
- Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
- Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
- Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
- Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
- Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
- Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
- Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.
- Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Automatyzacja

- Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
- Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
- Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
- Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.
- Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
- Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
- Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).

- Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
- Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.
- Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.
- Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.
- Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
- Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
- Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
- Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
- Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi
- Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
- Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.
- W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.
- Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie

makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)

- Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
- Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika
- Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
- Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)
- Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)
- Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)
- Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

Backup danych użytkownika

- Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
- Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
- Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.
- Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
- Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
- Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
- Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

Zarządzanie urządzeniami USB Storage

- Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.

- Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
- Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
- Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage
- Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

Monitoring stanowisk komputerowych

- Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
- Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
- Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
- Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
- Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
- Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
- Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
- Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
- Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
- Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
- Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
- Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
- Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
- Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB.

Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.

- Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.
- Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

Monitoring sieci LAN

- Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony
- Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.
- Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
- Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
- Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
- Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
- Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
- Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

Wymagania formalne:

- Dostarczone licencje na oprogramowanie muszą być bezterminowe.
- Dostarczone licencje na oprogramowanie muszą być dostarczone z 36 miesięcznym supportem producenta, liczonym od daty zakończenia wdrożenia.
- Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz gwarancji technicznej producenta.

- Dostarczone licencje na oprogramowanie muszą objąć co najmniej 60 stanowisk komputerowych z systemem klasy Microsoft Windows
- Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp).
- Ponadto musi posiadać co najmniej 2 licencje dostępowe do konsoli zarządzającej.
- W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.
- Zamawiający wymaga od wykonawcy, aby w terminie 20 dni od podpisania umowy przeprowadził wdrożenie systemu zdalnie (wymagane co najmniej 2 sesje – 5 godzinne)
- Zamawiający wymaga, aby producent oferowanego oprogramowania przedstawił potwierdzanie (certyfikat), że oprogramowanie wytwarzane jest zgodnie z normą ISO27001.

Wymagania dotyczące zgodności z najlepszymi praktykami ITSM.
Zamawiający wymaga, aby oferowane oprogramowanie w zakresie:

- Zarządzanie incydentami (Incident Management),
- Zarządzanie problemami (Problem Management),
- Zarządzanie bazą wiedzy (Knowledge Management),
- Zarządzanie zasobami (Asset Management).

posiadało aktualny certyfikat zgodności z najlepszymi praktykami IT Service Management, wydany przez niezależną organizację certyfikującą (np. Pink Elephant)

Do oferty należy dołączyć kopię stosownego certyfikatu oraz wskazać link do strony internetowej organizacji certyfikującej, na której potwierdzona jest zgodność oferowanego rozwiązania z ww. procesami ITSM.

Poz. 2. Oprogramowanie do kopii zapasowych

Ilość: licencja na 2 serwery fizyczne + maszyny wirtualne + 50 stacji roboczych, okres 36 miesięcy

Wymagania ogólne

- Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights i spełniać minimalne wymaganie: minimalna liczba referencji 500, minimalna ocena z referencji 4,6.
- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x, 8.x i 9.0 oraz Microsoft Hyper-V 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne dla powyższych platform wirtualizacyjnych, chyba że wyszczególniono inaczej.

- Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.8.x–7.3, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.5 lub nowszy, Proxmox VE 8.2–9.0 oraz Scale Computing HyperCore 9.4–9.5.x.
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
- System backupowy musi mieć możliwość wdrożenia wszystkich komponentów (serwer backupowy, serwer pośredniczący, repozytorium) na platformach Windows oraz Linux.
- System backupowy musi mieć możliwość wdrożenia w oparciu o tzw. appliance zgodny z wytycznymi bezpieczeństwa DISA (Defense Information Systems Agency).
- Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
- Oprogramowanie musi tworzyć „samowystarczalne" archiwa, do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
- Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć wiele wirtualnych puli pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej 20 pamięci masowych w pojedynczej puli.
- Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta.
- Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage, IBM Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
- Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
- Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania do backupu oraz odtwarzania obrazu maszyny wirtualnej.
- Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).
- Oprogramowanie musi umożliwiać tworzenie logicznie odseparowanych środowisk dla różnych organizacji/działów. Dodatkowo system musi wspierać kontrolę dostępu w oparciu o role (RBAC) — predefiniowane lub własne.
- Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.

- Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
- Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
- Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.
- Oprogramowanie musi umożliwiać integrację z różnymi dostawcami tożsamości (IdP — Identity Providers) z wykorzystaniem protokołu SAML (np. Entra ID, Okta).
- Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora, reset zablokowanego konta).
- Oprogramowanie musi posiadać integrację z systemami zarządzania kluczami szyfrującymi (KMS).
- Oprogramowanie musi posiadać integrację z systemami typu SIEM.
- Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej oraz analizy istniejącej instalacji systemu backupowego. Powinna istnieć możliwość wyłączenia tej opcji.
- Oprogramowanie musi pozwalać na wydawanie komend głosowych asystentowi AI.

Wymagania RPO

- Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware i Hyper-V.
- 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.
- Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
- Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
- Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016–2025 z systemem plików ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
- Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy

hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

- Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere lub dowolnego systemu operacyjnego Windows Server 2016/2025. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.
- Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
- Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).

Wymagania RTO

- Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
- Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w platformę. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności — oprogramowanie musi realizować taką migrację swoimi mechanizmami.
- Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny, zarówno fizycznej jak i wirtualnej.
- Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
- Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.
- Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.
- Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.
- Oprogramowanie musi wspierać bezagentowy backup, spójny aplikacyjnie (tzw. Application Consistent) dla maszyn wirtualnych z platform vSphere, Hyper-V, Nutanix AHV, Proxmox.

- Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej (minimum dla Active Directory, MS Exchange, MS SQL, MS SharePoint, Oracle i PostgreSQL).
- Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects oraz pozwalać na odtworzenie haseł.
- Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, enterprise applications, Conditional Access Policies, Intune Policies oraz logi audytowe i sign-in.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange (dowolny obiekt w tym obiekty w folderze „Permanently Deleted Objects”). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SharePoint. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
- Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
- Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
- Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
- Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.
- Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.
- Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.
- Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.
- Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2.
- Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym „reverse CBT” oraz odtwarzanie z wykorzystaniem sieci SAN.

Ograniczenie ryzyka

- Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

- Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych.
- Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.
- Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
- Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backupowych.
- Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.
- Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.
- Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning), musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.
- Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw. Indicators of Compromise.
- Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
- Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa — minimum Splunk, Palo Alto Networks XSOAR/XSIAM, CrowdStrike Falcon LogScale, Microsoft Sentinel.

Środowiska fizyczne

- Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.
- Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.
- Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Rocky Linux, AlmaLinux.
- Rozwiązanie musi wspierać system operacyjny macOS.
- Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix.
- Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).
- Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.

- Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery), wybranych wolumenów, oraz wybranych plików i folderów.
- Rozwiązanie musi wspierać backup podłączonych dysków USB.
- Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.
- Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), Network Attached Storage (NAS) poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury).
- Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.
- Rozwiązanie musi wspierać kontrolę pasma sieciowego.
- Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.
- Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.
- Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.
- Rozwiązanie musi wspierać technologię BitLocker.
- Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.
- Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange, Microsoft Active Directory, Microsoft SharePoint, Microsoft SQL, Oracle, PostgreSQL oraz MongoDB.
- Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.
- Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
- Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
- Rozwiązanie musi wspierać szyfrowanie.
- Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium jest niedostępne.
- Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.
- Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.
- Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.

Monitoring

- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 7.x–9.0 zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2016–2025 oraz Azure Stack HCI zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server.
- System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.
- System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
- System musi mieć wbudowaną bazę wiedzy opisującą problemy z predefiniowanych alarmów.
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (dashboard).
- System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
- System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
- System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
- System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych.
- System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom.

Raportowanie

- System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 7.x–9.0 oraz Microsoft Hyper-V 2016–2025.
- System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
- System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.

- System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Adobe PDF.
- System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
- System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
- System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
- System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
- System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
- System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach „what-if".
- System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom.
- System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
- System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.
- System musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej oraz analizy istniejącej instalacji systemu backupowego. Powinna istnieć możliwość wyłączenia tej opcji.

Poz. 3. Oprogramowanie DLP wraz ze wsparciem — pakiet 50 licencji

Ilość: licencja na 50 stacji roboczych z gwarancją na okres 36 miesięcy

Kluczowe funkcjonalności

- System umożliwia instalację na systemie operacyjnym Windows Server 20 i nowszym.
- Dostęp do systemu jest zapewniony za pośrednictwem konsoli webowej bez konieczności instalacji dodatkowych komponentów.
- System działa agentowo.
- System obsługuje bazy danych Postgres oraz MS SQL jako instancje do przechowywania danych.
- System posiada wbudowane funkcjonalności wykonywania backupu bazy danych, odtworzenia bazy danych, zmiany bazy danych.
- System pozwala na podłączenie certyfikatu w formie .PFX(PKCS12).

- System posiada interfejs programowania aplikacji API pozwalający na integrację z innymi systemami.
- System posiada możliwość zarządzania urządzeniami z systemami Windows 8 i nowsze.
- System posiada możliwość konfiguracji skrzynki pocztowej celem wysyłania alertów i raportów.
- System posiada wsparcie dla sieci: Active Directory, Grupy robocze, Wiele domen, Oddziały i biura zdalne
- System pozwala na konfigurację serwera Proxy.
- System pozwala na konfigurację NATu.
- System pozwala na bezpieczną pracę w sieci LAN i WAN.
- System zawiera przeglądarkę dziennika logów.
- System posiada możliwość konfiguracji w trybie Failover.

2. Wymagania podstawowe systemu

- System rozpoznaje stacje robocze w ramach Active Directory oraz Workgroup.
- System posiada możliwość tworzenia grup użytkowników lub komputerów.
- System posiada możliwość tworzenia grup na podstawie grup Active Directory.
- System posiada możliwość integracji z Active Directory.
- System posiada możliwość tworzenia ról z różnym poziomem uprawnień.
- System posiada możliwość przechowywania poświadczeń.

System posiada możliwość konfigurowania polis określających pliki jako posiadające dane wrażliwe:

- Dane finansowe.
- Dane zdrowotne.
- Dane osobowe.

System pozwala na tworzenie własnych reguł w oparciu o:

- Wzorce RegEx.
- Słowa kluczowe dla nazw plików.
- Nazwy dokumentów.
- Rozszerzenia plików.
- System pozwala na audytowanie dostępu do plików z danymi wrażliwymi.
- System pozwala na blokadę wykonywania zrzutów ekranu.
- System pozwala na audytowanie klienta pocztowego Outlook.
- System pozwala na określenie zaufanych domen, do których będzie możliwe wysłanie maila zawierającego dane wrażliwe.
- System pozwala na audytowanie przeglądarek i upload plików. Wspierane przeglądarki: Google Chrome, Microsoft Edge, Mozilla FireFox, Brave, Ulaa.
- System pozwala na określenie zaufanych domen, na które będzie możliwy upload plików.
- System pozwala na audytowanie urządzeń USB podłączanych do komputera.
- System pozwala na określenie zaufanych urządzeń UB, na które będzie możliwy transfer plików zawierających dane wrażliwe.
- System pozwala na audytowanie wydruków dla drukarek lokalnych oraz sieciowych.
- System pozwala na określenie zaufanych drukarek, na których możliwe będzie drukowanie plików zawierających dane wrażliwe.

- System pozwala na dodanie znaku wodnego do wydruku.
- System pozwala na oznaczanie fałszywych zagrożeń tzw. False Positive.

System posiada moduł raportowy pozwalający na:

- Tworzenie własnych raportów.
- Tworzenie raportów zaplanowanych.
- Tworzenie raportów w oparciu o zapytania SQL.

System posiada możliwość łatwej weryfikacji systemów, które mają już skonfigurowaną i wdrożoną politykę DLP.

Poz. 4. System do zbierania i analizy logów

Ilość: 1 szt. (maszyna wirtualna, pojemność 5 GB logów/dzień)

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 8.0/9.0, Microsoft Hyper-V 2019, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

Interfejsy, Dysk:

- System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.

Parametry wydajnościowe:

- System musi być w stanie przyjmować minimum 5 GB logów na dzień.
- Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

Logowanie

- Podgląd logowanych zdarzeń w czasie rzeczywistym.
- Możliwość przeglądania logów historycznych z funkcją filtrowania.
- System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
    1. Listę najczęściej wykrywanych ataków.

2. Listę najbardziej aktywnych użytkowników.
3. Listę najczęściej wykorzystywanych aplikacji.
4. Listę najczęściej odwiedzanych stron www.
5. Listę krajów, do których nawiązywane są połączenia.
6. Listę najczęściej wykorzystywanych polityk Firewall.
7. Informacje o realizowanych połączeniach IPSec.

- Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.

- Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.

- System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

- Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.

- Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.

- Funkcję definiowania własnych raportów.

- Możliwość spolszczenia raportów.

- Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

- Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.

- Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

- Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

    - Malware.
    - Aplikacje sieciowe.
    - Email.
    - IPS.
    - Traffic.

- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
- Automatyczne uruchomienia procesów odpowiedzi współpracujących systemów na wykryte w analizie korelacji logów zagrożenie.

Zarządzanie

- System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
- Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
- System musi umożliwiać zdefiniowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Gwarancja

- Gwarancja: System musi być objęty gwarancją producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz gwarancji technicznej w trybie 24x7. Rozwiązanie musi być dostarczone z licencją na wszystkie wymagane funkcjonalności w formie subskrypcji.

Opisy do wymagań ogólnych

- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Poz. 5. Oprogramowanie do zarządzania podatnościami — pakiet 50 licencji

Ilość: 1 instancja (licencja na minimum 50 assetów)

OPZ – System zarządzania podatnościami (on-prem, enterprise)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja systemu do zarządzania podatnościami w modelu **on-premise**, umożliwiającego identyfikację, analizę i raportowanie podatności w infrastrukturze IT Zamawiającego.

System musi być rozwiązaniem klasy vulnerability management, działającym lokalnie, bez konieczności korzystania z usług chmurowych.

2. Wymagania ogólne

- System musi:
  - być dostępny w formie **appliance (fizycznego lub wirtualnego)**
  - umożliwiać szybkie wdrożenie (plug-and-play)

- System musi umożliwiać:
  - pracę w środowiskach odizolowanych (air-gap)
  - aktualizację offline (bez dostępu do Internetu)
- System musi zapewniać:
  - pełną kontrolę nad danymi (lokalne przechowywanie wyników)

3. Architektura systemu

System musi:

- posiadać architekturę składającą się z:
  - komponentu zarządzającego (centralnego)
  - jednego lub wielu komponentów skanujących
- umożliwiać:
  - separację warstwy zarządzającej i skanującej
  - centralne zarządzanie wieloma silnikami skanującymi
- wspierać model:
  - master / sensor

4. Funkcjonalności skanowania

System musi:

- obsługiwać:
  - skanowanie aktywne (sieciowe)
  - skanowanie uwierzytelnione i nieuwierzytelnione
- umożliwiać:
  - wykrywanie podatności w systemach operacyjnych, usługach i urządzeniach sieciowych
  - definiowanie polityk skanowania
  - harmonogramowanie skanów
- wykorzystywać:
  - aktualizowaną bazę testów podatności

5. Baza podatności

System musi:

- wykorzystywać bazę podatności:
  - aktualizowaną co najmniej raz dziennie
- zawierać:
  - informacje o CVE

6. Analiza i raportowanie

System musi:

- umożliwiać:
  - generowanie raportów technicznych i zarządczych
  - analizę trendów podatności
  - filtrowanie wyników według CVSS
- obsługiwać eksport:
  - PDF

  - CSV
- posiadać:
  - dashboardy wizualizujące stan bezpieczeństwa

7. Zarządzanie użytkownikami

System musi:

- obsługiwać:
  - role i uprawnienia użytkowników
- umożliwiać:
  - integrację z LDAP/Active Directory
- rejestrować:
  - działania użytkowników

8. API i integracje

System musi:

- udostępniać API umożliwiające:
  - zarządzanie skanami
  - pobieranie wyników
- dopuszcza się API:
  - REST lub równoważne (np. XML-based)

9. Bezpieczeństwo i operacje

System musi:

- zapewniać:
  - szyfrowanie komunikacji
  - mechanizmy backupu
  - logowanie zdarzeń
- umożliwiać:
  - aktualizację systemu oraz bazy podatności

10. Licencjonowanie

System musi:

- umożliwiać:
  - licencjonowanie oparte na liczbie zasobów lub równoważne
- nie może wymagać:
  - dodatkowych opłat za kluczowe funkcjonalności (skanowanie, raportowanie, API)

11. Skalowalność

System musi:

- umożliwiać:
  - rozbudowę poprzez dodawanie kolejnych komponentów skanujących
- wspierać:
  - środowiska rozproszone

12. Wdrożenie i szkolenie

- instalacja i konfiguracja systemu
- szkolenie administratorów i użytkowników

Poz. 6. Oprogramowanie wspomagające zarządzanie ryzykiem, zgłaszanie incydentów i audyty

Ilość / zakres: 1 instancja systemu wspierającego zarządzanie ryzykiem, incydentami i audytami.

Przedmiot zamówienia

- Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja oprogramowania wspierającego zarządzanie ryzykiem, zgłaszanie i obsługę incydentów bezpieczeństwa, planowanie i dokumentowanie audytów oraz prowadzenie rejestrów kontrolnych i działań korygujących.

Zakres zamówienia

- Dostawa licencji/subskrypcji systemu GRC/zarządzania ryzykiem i incydentami.
- Instalacja i konfiguracja systemu lub udostępnienie instancji w modelu zgodnym z wymaganiami Zamawiającego.
- Konfiguracja podstawowych rejestrów ryzyk, incydentów, audytów, działań korygujących i raportów.
- Utworzenie ról i uprawnień administratorów oraz użytkowników zgłaszających incydenty.
- Instruktaż administratorów i przekazanie dokumentacji powdrożeniowej.

Minimalne wymagania techniczne

- System musi posiadać interfejs dostępny przez przeglądarkę WWW.
- System musi umożliwiać pracę co najmniej w języku polskim.
- System musi obsługiwać role i uprawnienia użytkowników, w tym administratora, operatora, audytora, właściciela ryzyka i użytkownika zgłaszającego.
- System musi umożliwiać rejestrowanie zmian w kluczowych rejestrach oraz identyfikację osoby dokonującej zmiany.
- System musi umożliwiać eksport danych i raportów co najmniej do PDF, CSV lub XLSX albo równoważnych formatów.
- System musi umożliwiać konfigurację słowników, statusów, kategorii, priorytetów i formularzy.
- System musi umożliwiać pracę lokalną lub w modelu zapewniającym bezpieczeństwo i kontrolę danych Zamawiającego.

Minimalne wymagania funkcjonalne

- Prowadzenie rejestru ryzyk, w tym opisu ryzyka, właściciela, kategorii, prawdopodobieństwa, skutku, poziomu ryzyka, zabezpieczeń i działań mitygujących.
- Definiowanie metodyki oceny ryzyka opartej co najmniej na macierzy prawdopodobieństwo-skutek lub równoważnym modelu punktowym.
- Prowadzenie rejestru incydentów bezpieczeństwa z możliwością określania kategorii, priorytetu, statusu, osoby odpowiedzialnej, terminu i działań podjętych.
- Udostępnienie formularza zgłaszania incydentów przez uprawnionych użytkowników.
- Obsługa procesu obsługi incydentu: rejestracja, kwalifikacja, analiza, działania, zamknięcie i raport.
- Prowadzenie planów audytów, list kontrolnych, ustaleń audytowych, niezgodności, zaleceń i działań korygujących.
- Przypisywanie zadań do osób odpowiedzialnych, określanie terminów i monitorowanie statusu realizacji.
- Raportowanie ryzyk, incydentów, audytów, zaleceń i działań korygujących.
- Możliwość załączania dokumentów, dowodów, zrzutów ekranu lub innych plików do wpisów w rejestrach.
- Możliwość prowadzenia historii zmian i komentarzy do wpisów.

Wymagania dotyczące bezpieczeństwa, zgodności i interoperacyjności

- System musi zapewniać szyfrowaną komunikację z interfejsem użytkownika.
- System musi ograniczać dostęp do danych według ról oraz umożliwiać separację informacji wrażliwych dotyczących incydentów.
- System musi rejestrować działania użytkowników w zakresie zmian w rejestrach, statusach i uprawnieniach.
- System musi zapewniać możliwość tworzenia kopii zapasowych danych lub udokumentowania sposobu objęcia danych backupem.
- System musi umożliwiać przechowywanie danych w lokalizacji zgodnej z wymaganiami Zamawiającego i przepisami dotyczącymi ochrony danych.

Wymagania dotyczące licencji i subskrypcji

- Licencja musi obejmować wszystkie wymagane rejestry i funkcje: ryzyka, incydenty, audyty, działania korygujące, raporty, role i eksport danych.
- Wykonawca musi wskazać liczbę użytkowników administracyjnych, operatorskich i zgłaszających objętych ofertą lub potwierdzić brak ograniczeń w tym zakresie.

- Licencja nie może wymagać dodatkowych opłat za funkcje wymagane w OPZ.

Dostawa, wdrożenie, konfiguracja i szkolenie

- Wykonawca dostarczy licencje, dane dostępowe, instalatory lub dostęp do instancji.
- Wykonawca skonfiguruje role, podstawowe słowniki, statusy, formularze, przykładowy rejestr ryzyk, rejestr incydentów, plan audytu i raport.
- Wykonawca przeprowadzi instruktaż administratorów z zakresu obsługi rejestrów, raportów, ról i workflow.

Dokumentacja, gwarancja i wsparcie techniczne

- Dokumentacja powdrożeniowa musi obejmować opis konfiguracji, ról, słowników, formularzy, rejestrów, procesu zgłaszania incydentów, backupu i raportowania.
- Wykonawca zapewni wsparcie techniczne przez okres wskazany w SWZ/ofertach.
- W okresie wsparcia Wykonawca zapewni dostęp do aktualizacji i poprawek producenta, o ile są dostępne.

Odbiór

- Odbiór nastąpi po aktywowaniu licencji, uruchomieniu systemu, utworzeniu przykładowego ryzyka, incydentu, audytu, działania korygującego oraz wygenerowaniu raportu.
- Warunkiem odbioru jest przekazanie dokumentacji i potwierdzenie przeszkolenia administratorów.

Warunki równoważności

- Za równoważne uznaje się rozwiązanie GRC lub równoważne narzędzie zarządzania ryzykiem, incydentami i audytami, które spełnia minimalne wymagania funkcjonalne i bezpieczeństwa.
- Dopuszcza się różne nazewnictwo modułów i procesów, pod warunkiem realizacji wymaganego efektu: rejestracja, analiza, przypisanie odpowiedzialności, raportowanie i historia zmian.

Informacje i dokumenty wymagane od Wykonawcy w ofercie

- Nazwa i wersja systemu oraz producent.
- Model licencjonowania i liczba użytkowników/administratorów.

Sprzęt IT

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa fabrycznie nowego, nieużywanego, kompletnego i gotowego do pracy sprzętu informatycznego, w tym sprzętu specjalistycznego, przeznaczonego do podniesienia poziomu bezpieczeństwa, niezawodności oraz ciągłości działania infrastruktury teleinformatycznej Zamawiającego.

Zamówienie obejmuje dostawę sprzętu wraz z niezbędnymi akcesoriami, licencjami, oprogramowaniem układowym, dokumentacją, gwarancją producenta oraz czynnościami instalacyjnymi i konfiguracyjnymi wskazanymi w niniejszym OPZ. Wykonawca zobowiązany jest dostarczyć rozwiązania kompletne, legalne, pochodzące z autoryzowanego kanału dystrybucji oraz możliwe do zarejestrowania u producenta na Zamawiającego.

Cel zamówienia

Część II. Sprzęt IT

Celem zamówienia jest wzmocnienie infrastruktury IT Zamawiającego poprzez zapewnienie odpowiedniego poziomu ochrony sieci, bezpiecznego przechowywania i odtwarzania danych, stabilnego zasilania awaryjnego, wydajnej infrastruktury serwerowej oraz zarządzalnej infrastruktury przełączającej. Dostarczony sprzęt ma wspierać realizację zadań publicznych, zapewnić większą odporność na incydenty cyberbezpieczeństwa oraz umożliwić utrzymanie usług informatycznych na poziomie wymaganym dla jednostki administracji publicznej.

Zakres zamówienia

Lp.	Nazwa kategorii	Minimalna ilość	Charakter dostawy
1	UPS centralny	1 szt.	zasilanie awaryjne infrastruktury centralnej (szafa rack)
2	UPS do stacji roboczych 50 szt.	50 szt.	zasilanie awaryjne stanowisk roboczych
3	Serwery 2 szt.	2 szt.	infrastruktura serwerowa do wirtualizacji i usług lokalnych
4	Switche większe 5 szt.	5 szt.	przełączniki zarządzalne o większej liczbie portów
5	Switche mniejsze 10 szt.	10 szt.	przełączniki zarządzalne dostępowe
6	Urządzenie UTM	2 szt.	ochrona brzegu sieci i usługi bezpieczeństwa
7	NAS 2 szt.	2 kpl.	urządzenia do przechowywania danych i backupu

Ogólne wymagania dla całości zamówienia

Wykonawca zobowiązany jest dostarczyć sprzęt spełniający co najmniej wymagania minimalne określone w niniejszym OPZ. Parametry zaoferowane przez Wykonawcę nie mogą być gorsze od

parametrów wymaganych. Dopuszcza się zaoferowanie sprzętu o parametrach równoważnych lub lepszych, pod warunkiem zachowania pełnej funkcjonalności, kompatybilności oraz możliwości wdrożenia w środowisku Zamawiającego.

- Sprzęt musi być fabrycznie nowy, nieużywany, kompletny, sprawny technicznie, wolny od wad fizycznych i prawnych oraz niewycofany z oficjalnej dystrybucji producenta na dzień składania oferty.
- Dostarczone urządzenia muszą pochodzić z legalnego kanału sprzedaży, a Zamawiający musi mieć możliwość uzyskania wsparcia gwarancyjnego producenta lub autoryzowanego serwisu.
- Wszystkie elementy wymagające licencji, subskrypcji, aktywacji lub rejestracji muszą zostać dostarczone w zakresie umożliwiającym korzystanie z pełnej funkcjonalności wymaganej w OPZ przez okres wskazany przy danej kategorii.
- Wykonawca odpowiada za kompletność dostawy, w tym za dostarczenie przewodów zasilających, elementów montażowych rack, uchwytów, szyn, modułów, wkładek, nośników, licencji i dokumentacji, jeżeli są niezbędne do uruchomienia sprzętu zgodnie z przeznaczeniem.
- Dostarczony sprzęt musi być zgodny z obowiązującymi przepisami prawa, normami bezpieczeństwa, wymaganiami kompatybilności elektromagnetycznej oraz wymaganiami producenta dotyczącymi eksploatacji.
- W przypadku użycia przez Zamawiającego w OPZ nazw technologii, standardów lub funkcjonalności powszechnie przyjętych na rynku, należy je rozumieć jako określenie klasy rozwiązania i minimalnego poziomu funkcjonalnego, a nie jako wskazanie konkretnego producenta.

Poz. 1. UPS centralny

Ilość: 1 szt.

Opis zasilacza UPS o mocy 10 000 VA (10 kW).

Tabela 1.1. Minimalne parametry UPS

PARAMETR	CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ
Minimalne wymagania techniczne dla jednostki UPS	• Moc znamionowa jednostki nie mniej niż 10 kVA / 10 kW • Konfiguracja faz 1:1 • Jednostka w obudowie uniwersalnej, umożliwiająca montaż w pozycji rack 5U oraz tower • Technologia Podwójnej konwersji (online), • Temperatura pracy 0 - 40 °C • Wilgotność względna 0 - 95 % bez kondensacji

	• Wysokość n.p.m. podczas pracy do 3000 m • Hałas słyszalny w odległości 1 m <55dBA • Sprawność do 95% w trybie online oraz do 98% w trybie ECO • Klasa ochrony IP 20 • Max. wymiary (szer. x wys. x gł.) w mm: 430 x 217 x 630 • Max. masa produktu: 75 kg
Parametry zasilania wejściowego	• Nominalne napięcie wejściowe 230V • Częstotliwość 50 / 60Hz • Zakres częstotliwości wejściowej 40 - 70 Hz (wykrywanie automatyczne) • Typ gniazda wejściowego: listwa zaciskowa • Zakres napięcia wejściowego 176 – 288 VAC (100 do 176VAC przy obniżeniu wartości znamionowych)
Parametry zasilania wyjściowego	• Napięcie wyjściowe 230V AC • Inne napięcia wyjściowe 200/208/220/240 • Typ przebiegu: sinusoida • Złącza/gniazda wyjściowe - 4x IEC 320 C13 - 4x IEC 320 C19 - Listwa zaciskowa • Bypass wewnętrzny (automatyczny) i bypass serwisowy (POD) • Przeciążenie sieci (AC): >150% przez 200 ms; 125-150% przez 60 sekund; 105−125% przez 5 min; <105% kontynuacja pracy
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy, szczelny akumulator kwasowo-ołowiowy • Min. 16 akumulatorów 12V / 9Ah (jednostka UPS) • Czas autonomii: ≥ 2 minut dla pełnego obciążenia ≥ 7 minut dla połowy obciążenia • Możliwość podłączenia do 10 zewnętrznych modułów bateryjnych

	• Baterie wymieniane podczas pracy urządzenia (hot swap) • Prąd ładowania: nominalny:2.25A; maksymalny 8A
Komunikacja i zarządzanie	• Wbudowane porty komunikacyjne: RS232 Serial, DB9 do pracy równoległej, RS485 dla czujników środowiskowych, USB, blok styków bezpotencjałowych z funkcją zdalnego wyłączenia zasilacza REPO. • Karta sieciowa do zarządzania SNMP i siecią, posiadająca porty komunikacyjne: RJ-45, złącze czujników środowiskowych, USB • Panel sterowania: wielofunkcyjna konsola sterownicza w postaci kolorowego ekranu LCD z detekcją położenia, • Alarm: alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia • Darmowe oprogramowanie do zamykania systemów operacyjnych
Certyfikaty, zgodności oraz gwarancja	• Odporność na przepięcia IEC/EN EN61000-4-5 • Bezpieczeństwo IEC62040-1:wersja 2008, znak GS • Emisje IEC/EN/AS 62040-2, II wyd. (kat. 2) • 3 lata gwarancji na urządzenie oraz akumulator

Poz. 2. UPS do stacji roboczych 50 szt.

Ilość: 50 szt.

Opis zasilacza UPS o mocy 1000 VA (625 W).

Tabela 1.1. Minimalne parametry UPS

PARAMETR	**CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ**
Minimalne wymagania techniczne dla jednostki UPS	• Moc znamionowa jednostki nie mniej niż 1000VA / 625W • Jednostka w obudowie tower • Topologia line-interactive • Temperatura pracy 0 - 40 °C • Temperatura przechowywania -20 °C do +40 °C • Wilgotność względna 0 - 95% bez kondensacji • Wysokość n.p.m. podczas pracy do 3000 m • Słyszalny poziom hałasu: <40dBA w odległości 1m

	• Sprawność ≥ 95% przy pełnym obciążeniu • Waga max. jednostki - 10 kg
Parametry wejściowe	• Nominalne napięcie wejściowe 220-240V_{AC} • Zakres napięcia wejściowego 140 - 290V_{AC} • Częstotliwość 50/60Hz +/- 5Hz (wykrywanie automatyczne) • Typ gniazda wejściowego: IEC60320 C14 • Ochrona przed przepięciami: 600J
Parametry wyjściowe	• Napięcie wyjściowe 220-240V_{AC} • Zakres napięcia wyjściowego 195-255V_{AC} • Zakres częstotliwości: 50/60Hz +/-1 Hz • Złącza/gniazda wyjściowe: 4x Schuko • Typowy czas przełączania: 2-6 ms (maks. 10ms) • Elektroniczna ochrona przed przeciążeniem, zwarciem, przeładowaniem • Typ przebiegu: symulowana sinusoida • Przeciążalność: 110% przez 5 sek.; 120% natychmiastowe wyłączenie;
Akumulatory i czas podtrzymania	• Typ akumulatora: ołowiowo-kwasowy • Min. 2 akumulatory 12V x 7Ah • Czas autonomii: ≥ 2 min. 15sek. dla pełnego obciążenia ≥ 9 min. dla połowy obciążenia
Komunikacja i zarządzanie	• Wbudowany port komunikacyjny USB • Ochrona linii ethernet • Ciekłokrystaliczny wyświetlacz LCD ze wskaźnikami: - Statusu pracy urządzenia - Stanu naładowania baterii - Obciążenia urządzenia - Parametrami pracy min. Hz / kW / napięcie wejścia i wyjścia / napięcie akumulatora / przybliżony czas podtrzymania

	• Wymagane przyciski: zasilanie, wyciszenie, nawigacja LCD • Bezpłatne i dostępne do pobrania na stronie producenta oprogramowanie umożliwiające automatyczne wyłączenie systemu podczas przerwy w zasilaniu.
Certyfikaty, zgodności oraz gwarancja	• CE, RoHS, REACH, WEEE, EN/IEC 62040-1, EN/IEC 62040-2, EN/IEC 61000-3-2, EN 61000-3-3, IEC 61000-4-5 • 3 lata gwarancji

Poz. 3. Serwery 2 szt.

Zamówienie obejmuje dwa serwery w dwóch konfiguracjach opisanych poniżej.

Ilość: 2 szt.

5.1. Obudowa

- Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U
- Zestaw szyn do mocowania w szafie i wysuwania do celów serwisowych
- Możliwość instalacji ramienia do zarządzania kablami

5.2. Procesor

- Architektura x86
- Maksymalny TDP: 210W
- Wymagana ilość rdzeni: 24
- Minimalna częstotliwość pracy: 2.4 GHz
- Minimalna ilość kanałów procesora: 8
- Ilość kości pamięci na kanał: 2
- Wynik wydajności procesora nie powinien być niższy niż 521 punktów base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org), dla serwera oferowanego producenta

5.3. Liczba zainstalowanych procesorów

- 1 szt.

5.4. Płyta główna

- Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera
- Możliwość zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje

5.5. Pamięć operacyjna

- min. 128 GB DDR5 6400 MHz, zainstalowana w modułach 16 GB
- Pamięć zainstalowana w kościach 16 GB
- Minimum 32 sloty na pamięć
- Możliwość rozbudowy do 8 TB RAM

5.6. Zabezpieczenie pamięci

- Memory mirroring, ECC, SDDC, ADDDC

5.7. Procesor graficzny

- Zintegrowana karta graficzna z minimum 16 MB pamięci
- Rozdzielczość 1920x1200 przy 60 Hz

5.8. Rozbudowa dysków

- Serwer wyposażony w min. 8 zatok 2,5” obsługujących dyski SAS/SATA
- Kontroler RAID obsługujący poziomy RAID 0, 1, 10, 5, 6, 50, 60:
    - Wspierający dyski SED
    - Wyposażony w min. 4 GB pamięci cache
    - Nie zajmujący zewnętrznych slotów PCIe
- Zainstalowane min. 4 dyski 960 GB SATA 6Gb/s, Read Intensive, hot-swap
- Możliwość instalacji minimum 2 sztuk dysków M.2 i dedykowanego kontrolera sprzętowego umożliwiającym redundancję RAID-1
- Wymagany jest wewnętrzny slot na kartę Micro SD

5.9. Zasilacz

- Minimum dwa redundantne zasilacze o mocy minimum 1300W
- Certyfikat minimum Titanium
- Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji

5.10. Interfejsy sieciowe

- Zainstalowana przynajmniej jedna czteroportowa karta 1 Gb RJ-45 nie zajmująca slotów PCIe
- Jeden port RJ-45 o przepustowości 1 GbE dedykowany dla karty zarządzającej

5.11. Sloty I/O

- 2 sloty PCIe Gen5 x16 (z czego jeden slot pełnej wysokości)
- 2 sloty OCP Gen5 (min. jeden aktywny)
- Dedykowane połączenie PCIe dla kontrolera dyskowego niezajmujące slotów PCIe

5.12. Dodatkowe porty

Z przodu obudowy:

- 2x USB 3 (z czego jeden z możliwością zarządzania serwerem)
- Port Mini DisplayPort
- Zewnętrzny dedykowany port diagnostyczny

Z tyłu obudowy:

- 2x USB 3
- 1x VGA

- 1x RJ-45 do zarządzania serwerem
- Możliwość instalacji portu DB9

Wewnątrz obudowy:

- Port USB 3

Rozwiązanie, w którym wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port na kartę Micro SD będą umieszczone na osobnej dedykowanej płytce I/O łączonej bezpośrednio z płytą główną serwera, będzie dodatkowo punktowane.

5.13. Chłodzenie

- Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1

5.14. Zarządzanie

Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe porty):

- Monitoring stanu systemu (CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)
- Pozyskanie informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, utylizacja CPU, pamięci oraz komponentów I/O, lokalizacja
- Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika (min. 1024 rekordów na dziennik)
- Logowanie zdarzeń związanych z utrzymaniem systemu (upgrade firmware, zmiana/instalacja sprzętu) — min. 250 zdarzeń
- Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3
- Update systemowego firmware
- Monitoring i możliwość ograniczenia poboru prądu
- Zdalne włączanie/wyłączanie/restart
- Zapis video zdalnych sesji
- Podmontowanie lokalnych mediów z wykorzystaniem Java client
- Przekierowanie konsoli szeregowej przez IPMI
- Zrzut ekranu w momencie zawieszenia systemu
- Możliwość przejęcia zdalnego ekranu
- Możliwość zdalnej instalacji systemu operacyjnego
- Alerty Syslog
- Przekierowanie konsoli szeregowej przez SSH
- Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera
- Możliwość mapowania obrazów ISO z lokalnego dysku operatora
- Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
- Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
- Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API

- Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z kartą zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.
- Kontroler zarządzania musi umożliwiać uzyskanie 4 GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.
- Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany — zapis w logu serwera lub uniemożliwienie boot'u.
- Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.
- Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera (min. 200 serwerów).

Możliwość dostarczenia z serwerem dodatkowego oprogramowania zarządzającego umożliwiającego:

- Zarządzanie infrastrukturą serwerów i storage bez udziału dedykowanego agenta
- Przedstawianie graficznej reprezentacji zarządzanych urządzeń
- Możliwość skalowania do minimum 1000 urządzeń
- Obsługa szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2
- Wsparcie dla certyfikatów SSL (self-signed oraz zewnętrznych)
- Udostępnianie szybkiego podglądu stanu środowiska
- Udostępnianie podsumowania stanu dla każdego urządzenia
- Tworzenie alertów przy zmianie stanu urządzenia
- Monitorowanie oraz tracking zużycia energii (możliwość ustalania granicy zużycia)
- Konsola zarządzania oparta o HTML 5
- Dostępność konsoli monitorującej na urządzeniach przenośnych (Android oraz iOS) z możliwością: włączenia/wyłączenia/restartu urządzenia, aktywacji diody lokacyjnej
- Automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja
- Możliwość podnoszenia wersji oprogramowania komponentów w oparciu o repozytorium lokalne jak i zdalne (strona producenta)
- Definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń
- Definiowanie ról użytkowników oprogramowania
- Obsługa REST API oraz Windows PowerShell
- Obsługa SNMP, SYSLOG, Email Forwarding
- Autentykacja użytkowników: centralna (definiowanie poziomu skomplikowania), integracja z MS AD, single sign on, SAML
- Obsługa Forward Secrecy w komunikacji z zarządzanymi urządzeniami
- Przedstawianie historycznych aktywności użytkowników
- Blokowanie możliwości podłączenia innego systemu zarządzania do zarządzanych urządzeń
- Tworzenie dziennika zdarzeń (ukończone sukcesem/błędem, w trakcie). Możliwość definiowania filtrów i eksportu do pliku CSV
- Obsługa NTP

- Przesyłanie alertów do konsol firm trzecich
- Tworzenie wzorców konfiguracji (definiowanie przez konsolę lub kopiowanie z istniejących)
- Instalowanie systemów operacyjnych oraz wirtualizatorów VMware i Hyper-V. Wymagana integracja konsoli zarządzania z konsolą wirtualizatora. Min. 20 nodów jednocześnie
- Możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta wraz z przesyłem plików diagnostycznych

Producent serwera powinien mieć w ofercie narzędzia integrujące zarządzanie infrastrukturą z: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.

5.15. Funkcje zabezpieczeń

- Możliwość zainstalowania czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem
- Hasło włączania, hasło administratora
- Moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)
- Możliwość zainstalowania przedniego panelu zamykanego na klucz
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania
- Możliwość włączania i wyłączania portów USB na obudowie z poziomu karty zarządzania
- Możliwość wymazania danych z dysków wewnątrz serwera — niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem
- Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej
- Automatyczne przywrócenie BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji

5.16. Urządzenia hot swap

- Dyski twarde, zasilacze, wentylatory

5.17. Obsługa

- Możliwość instalacji serwera oraz serwisowania komponentów (risery PCIe, backplane’y dysków, karty rozszerzeń, wentylatory) bez użycia dodatkowych narzędzi mechanicznych

5.18. Diagnostyka

- Możliwość przewidywania awarii dla: procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID

5.19. Systemy operacyjne

- Microsoft Windows Server 2022, 2025
- Red Hat Enterprise Linux 9.x
- SUSE Linux Enterprise Server 15 SP6
- VMware vSphere (ESXi) 8.0 U3
- Ubuntu 22.04, 24.04

Wraz z serwerem powinno zostać dostarczone oprogramowanie Microsoft.

5.20. Waga

- Maksimum: 20 kg

5.21. Gwarancja

- Minimum 12 miesięcy gwarancji producenta, czas reakcji NBD
- Możliwość wykupienia dodatkowego wsparcia z gwarantowanym czasem naprawy w ciągu 24 godzin
- W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka — wymagane dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagane powyżej maszyny
- Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera

5.23. Licencje Microsoft

Produkt	Ilość
Windows Server 2025 Standard ROK (16 core) — MultiLang	2
Windows Server 2025 Standard Additional License (2 core)	8
Windows Server 2025 CAL (50 Device)	1
Windows Server 2025 Remote Desktop Services CAL (1 Device)	1

Poz. 4. Switche większe 5 szt.

Ilość: 5 szt.

Przełącznik sieciowy 48-portowy.

- Parametry fizyczne platformy:
- wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U
- Zasilanie 230V
- MTBF > 10lat
- Interfejsy sieciowe – wymagania minimalne:
- 48 portów GE, RJ-45
- 4 porty 10GE SFP+
- 24 porty umożliwiających zasilanie PoE 802.3af/at o sumarycznym budżecie mocy 370W – dla wersji z POE

- 48 portów umożliwiających zasilanie PoE 802.3af/at o sumarycznym budżecie mocy 740W – dla wersji z FPOE

3. Zarządzanie:

- port konsoli szeregowej RJ45
- Zarządzanie przez wiersz poleceń (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę
- Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniami NGFW (Next Generation Firewall)
- Kontroler przełączników musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.
- Kontroler przełączników musi umożliwiać aktualizację oprogramowania zarządzanych przełączników
- Z poziomu kontrolera musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).
- Kontroler musi oferować możliwość automatycznej instalacji wskazanej wersji oprogramowania układowego firmware, po podłączeniu przełącznika. Oprogramowanie przełącznika, musi być przechowywane na kontrolerze.
- Parametry wydajnościowe:
- przepustowość urządzenia - min. 176 Gbps, min. 260 Mpps
- możliwość zapamiętania co najmniej 32 000 adresów MAC
- Opóźnienie - poniżej 1 mikrosekundy
- Bufor pakietów: min. 2 MB
- Pamięć DRAM: min. 512 MB
- Pamięć FLASH: min. 64 MB

5. Wymagane funkcje:

- możliwość automatycznej negocjacji prędkości i duplexu dla połączeń
- obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)
- możliwość agregacji portów zgodna z 802.3ad
- obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
- możliwość wykonywania routingu statycznego (realizowany software’owo)

- port-mirroring
- Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius
- zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru)
- możliwość zarządzania przez interfejs graficzny i tekstowy
- możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI
- możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:
    - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników
    - obsługa białych i czarnych list MAC
    - stateful firewall, umożliwiający kontrolę dostępu do sieci
    - routing statyczny i dynamiczny, co najmniej OSPF

6. Moduły sieciowe:

Wraz z przełącznikami należy dostarczyć następujące moduły sieciowe:

- Moduły 1GE SFP transceiver module, XXX – XX szt.
- Moduły 10GE SFP+ transceiver module, XXX – XX szt.

Moduły muszą być oficjalnie wspierane przez producenta urządzeń.

7. Gwarancja:

- Dożywotnia Gwarancja: urządzenia muszą być objęte dożywotnią producenta, gwarantującą wymianę wadliwego sprzętu (okres 5 lat od ogłoszenia zakończenia produkcji).
- Gwarancja: System powinien być objęty gwarancją producenta przez okres 36miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.
- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu, 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.

- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

Poz. 5. Switche mniejsze 10 szt.

Ilość: 10 szt.

Przełącznik sieciowy 8-portowy.

- Parametry fizyczne platformy:
- wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U
- Zasilanie 230V
- MTBF > 10lat
- Konstrukcja urządzenia chłodzona pasywnie (bez wentylatorów)
- Interfejsy sieciowe – wymagania minimalne:
- 7 portów GE, RJ-45
- 1 port GE POE PD RJ-45
- 2 porty 1GE SFP
- 8 portów GE RJ-45 umożliwiających zasilanie PoE 802.3af/at o sumarycznym budżecie mocy 65W – dla wersji z POE
- 8 portów GE RJ-45 umożliwiających zasilanie PoE 802.3af/at o sumarycznym budżecie mocy 130W – dla wersji z FPOE

3. Zarządzanie:

- port konsoli szeregowej RJ45
- Zarządzanie przez wiersz poleceń (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę
- Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniami NGFW (Next Generation Firewall)
- Kontroler przełączników musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.
- Kontroler przełączników musi umożliwiać aktualizację oprogramowania zarządzanych przełączników

- Z poziomu kontrolera musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).
- Kontroler musi oferować możliwość automatycznej instalacji wskazanej wersji oprogramowania układowego firmware, po podłączeniu przełącznika. Oprogramowanie przełącznika, musi być przechowywane na kontrolerze.
- Parametry wydajnościowe:
- przepustowość urządzenia - min. 20 Gbps, min. 30 Mpps
- możliwość zapamiętania co najmniej 8 000 adresów MAC
- Opóźnienie - poniżej 4,1 mikrosekundy
- Bufor pakietów: min. 512 KB
- Pamięć DRAM: min. 256 MB DDR3
- Pamięć FLASH: min. 32 MB

5. Wymagane funkcje:

- możliwość automatycznej negocjacji prędkości i duplexu dla połączeń
- obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)
- możliwość agregacji portów zgodna z 802.3ad
- obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
- możliwość wykonywania routingu statycznego (realizowany software'owo)
- port-mirroring
- Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius
- zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru)
- możliwość zarządzania przez interfejs graficzny i tekstowy
- możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI
- możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:
    - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników
    - obsługa białych i czarnych list MAC
    - stateful firewall, umożliwiający kontrolę dostępu do sieci
    - routing statyczny i dynamiczny, co najmniej OSPF

6. Moduły sieciowe:

Wraz z przełącznikami należy dostarczyć następujące moduły sieciowe:

- Moduły 1GE SFP transceiver module, XXX – XX szt.
- Moduły 10GE SFP+ transceiver module, XXX – XX szt.

Moduły muszą być oficjalnie wspierane przez producenta urządzeń.

7. Gwarancja:

- Dożywotnia Gwarancja: urządzenia muszą być objęte dożywotnią producenta, gwarantującą wymianę wadliwego sprzętu (okres 5 lat od ogłoszenia zakończenia produkcji).
- Gwarancja: System powinien być objęty gwarancją producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.
- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu, 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.
- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

Poz. 6. Urządzenie klasy UTM

Ilość: 2 szt. (klaster)

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji

programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

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

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

- System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
- 8 portami Gigabit Ethernet RJ-45.
- 2 gniazdami SFP+ 10 Gbps.
- System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

- W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.
- Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.

- Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.7 Gbps.
- Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps.
- 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 4.4 Gbps.
- Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.2 Gbps.
- Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.6 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

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

Polityki, Firewall

- Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
- Translację jeden do jeden oraz jeden do wielu.
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

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

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

Połączenia VPN

- System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
- Wsparcie dla IKE v1 oraz v2.
- Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19, 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.
- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

- Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

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

Ochrona przed atakami

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

- Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

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

Kontrola WWW

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

- System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

- System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
- System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
- System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
- Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

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

Logowanie

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

Testy wydajnościowe oraz funkcjonalne

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

Serwisy i licencje

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

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

Gwarancja

- System jest objęty gwarancją producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz gwarancja techniczna w trybie 24x7.

Opisy do wymagań ogólnych

- 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, 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.

- Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Poz. 7. NAS 2 szt.

Ilość: 2 kpl. (każdy komplet: 1 serwer NAS + 4 dyski 8 TB + 1 zestaw szyn rack)

W skład każdego kompletu wchodzi:

- 1x serwer NAS
- 1x zestaw szyn rack
- 4x dysk 8 TB
- 1x gwarancja producenta lub autoryzowanego partnera: 3 lata KYHD, SLA 5/13, reakcja NBD

7.1. Parametry ogólne

Parametr	Wymagania
Typ urządzenia	Serwer NAS
Obudowa	Rack 2U
Procesor	Czterordzeniowy, taktowanie min. 2,2 GHz
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	Min. 4 GB ECC SODIMM, rozszerzalna do min. 32 GB
Wentylatory	Min. 3 szt., wymienne
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe	Min. 1x 4-liniowe gniazdo x8 gen. 3

7.2. Możliwości rozbudowy

- Min. 8 kieszeni na dyski twarde hot-swap dostępnych w obudowie urządzenia, bez konieczności stosowania jednostek rozszerzających
- Możliwość dalszej rozbudowy pojemności przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej

7.3. Dyski twarde

- 4 szt. dysków 3.5” przystosowanych do pracy ciągłej
- Interfejs SATA, pojemność min. 8 TB
- Prędkość przesyłu danych: min. 281 MB/s
- MTBF: min. 1 200 000 godz.
- Cache: 512 MB
- Dyski tego samego producenta co macierz główna (kompatybilność na poziomie systemu operacyjnego oraz możliwość aktualizacji firmware z poziomu systemu NAS)

7.4. Porty zewnętrzne

- Min. 2x USB 3.2.1

- Min. 1x eSATA (jako gniazdo rozszerzenia)

7.5. Porty sieciowe

- Min. 4x 1 GbE RJ45 (z obsługą Link Aggregation / przełączania awaryjnego)

7.6. System plików

- Wewnętrzny: Btrfs, ext4
- Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT

7.7. Obsługiwane typy macierzy RAID

- SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10

7.8. Zarządzanie pamięcią masową

- Maksymalny rozmiar pojedynczego wolumenu: 108 TB
- Min. 64 wewnętrzne wolumeny
- Min. 64 obiekty iSCSI Target
- Min. 128 jednostek iSCSI LUN
- Obsługa klonowania/migawek jednostek iSCSI LUN

7.9. Obsługiwane protokoły

- SMB1 (CIFS), SMB2, SMB3
- NFSv3, NFSv4, NFSv4.1, sesje Kerberized NFS
- iSCSI, HTTP, HTTPS, FTP
- SNMP, LDAP, CalDAV

7.10. Konta i foldery współdzielone

- Min. 1 024 konta użytkowników
- Min. 256 grup użytkowników
- Min. 256 folderów współdzielonych
- Min. 8 zadań synchronizacji folderów współdzielonych

7.11. Usługi plików

- Protokoły plików: SMB, AFP, NFS, FTP, WebDAV, Rsync
- Min. 130 połączeń SMB (oparta o FSCT)
- Integracja z listą kontroli dostępu Windows (ACL)
- Uwierzytelnianie Kerberos NFS

7.12. Wirtualizacja

- VMware vSphere with VAAI
- Windows Server 2022
- Citrix Ready
- OpenStack

7.13. Bezpieczeństwo

- Zapora sieciowa
- Szyfrowanie folderów współdzielonych
- Szyfrowanie SMB
- FTP przez SSL/TLS, SFTP, rsync przez SSH

- Automatyczne blokowanie logowania
- Wsparcie Let's Encrypt
- HTTPS (konfigurowalny zestaw szyfrów)

7.14. Oprogramowanie

System plików i ochrona danych:

- Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików z obsługą migawek, sum kontrolnych CRC oraz lustrzanych kopii metadanych (zapewnienie integralności danych)
- Limit dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych
- Funkcja WORM (Write Once, Read Many) oraz migawki niezmienne

Kopie zapasowe:

- Darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych dla heterogenicznych środowisk IT
- Zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym centralnym interfejsie administratora
- Replikacja danych: lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe w chmurach publicznych (darmowe narzędzie z Centrum Pakietów)

Wysoka dostępność (HA):

- Tryb klastra wysokiej dostępności — 2 identyczne urządzenia jako jeden spójny system
- Dane z serwera aktywnego kopiowane na bieżąco do serwera pasywnego (replikacja w czasie rzeczywistym)
- Natychmiastowy dostęp do danych i usług w przypadku uszkodzenia jednostki aktywnej

7.15. Konserwacja

- Przesuwne szyny rack do wygodnej konserwacji urządzenia

7.16. Gwarancja

- 3 lata na całość sprzętu wraz z pozostawieniem dysków w miejscu instalacji po awarii (KYHD)
- Zgłoszenia serwisowe (SLA): 5/13 (5 dni w tygodniu, 13 godzin dziennie)
- Czas reakcji: Next Business Day (NBD)
- Świadczone przez podmiot posiadający oficjalną akredytację (certyfikat) producenta sprzętu głównego
- Wymagane przedstawienie dokumentu potwierdzającego akredytację

Część III. Wymagania dotyczące dostawy, wdrożenia, gwarancji i odbioru

Wymagania dotyczące dostawy

Dostawa zostanie zrealizowana do miejsca wskazanego przez Zamawiającego. Wykonawca odpowiada za transport, rozładunek, wniesienie sprzętu, zabezpieczenie urządzeń przed uszkodzeniem oraz przekazanie sprzętu osobom upoważnionym przez Zamawiającego. Ryzyko przypadkowej utraty lub uszkodzenia sprzętu przechodzi na Zamawiającego dopiero po podpisaniu protokołu odbioru bez zastrzeżeń.

- Sprzęt musi zostać dostarczony w oryginalnych opakowaniach producenta, z widocznymi numerami seryjnymi, jeżeli producent oznacza nimi urządzenia.
- Wykonawca przekaże wykaz dostarczonych urządzeń z numerami seryjnymi, modelami, okresem gwarancji oraz informacją o sposobie zgłoszeń serwisowych.
- Wykonawca dostarczy wszystkie elementy niezbędne do uruchomienia urządzeń zgodnie z OPZ, nawet jeżeli nie zostały osobno wymienione, ale są wymagane przez producenta lub wynikają z charakteru sprzętu.
- Dostawa częściowa jest dopuszczalna wyłącznie za zgodą Zamawiającego i nie może utrudniać odbioru ani wdrożenia całości rozwiązania.

Wymagania dotyczące instalacji, konfiguracji i uruchomienia

Zakres instalacji i konfiguracji powinien obejmować czynności niezbędne do potwierdzenia, że dostarczony sprzęt jest kompletny, sprawny i gotowy do dalszej konfiguracji produkcyjnej. Wykonawca nie powinien pozostawiać urządzeń w stanie uniemożliwiającym ich bezpieczne wykorzystanie przez Zamawiającego.

Kategoria	**Minimalny zakres czynności Wykonawcy**
UPS centralny	Montaż lub ustawienie, podłączenie, test pracy, sprawdzenie stanu baterii i przekazanie zaleceń eksploatacyjnych.
UPS do stacji roboczych 50 szt.	Dostawa do Zamawiającego, kontrola kompletności, przekazanie instrukcji i informacji o zasadach eksploatacji baterii.
Serwery 2 szt.	Montaż w rack, aktualizacja firmware, konfiguracja RAID, uruchomienie zarządzania zdalnego i test podstawowy.
Switche większe 5 szt.	Montaż, uruchomienie, nadanie podstawowych adresów zarządzających, aktualizacja firmware i test portów.
Switche mniejsze 10 szt	Uruchomienie testowe, aktualizacja firmware, przygotowanie do konfiguracji VLAN według potrzeb Zamawiającego.
Urządzenie UTM 2 szt.	Rejestracja licencji, aktualizacja oprogramowania, konfiguracja podstawowa interfejsów, kont administracyjnych i logowania.
NAS 2 szt.	Inicjalizacja, aktualizacja oprogramowania, konfiguracja RAID, utworzenie kont administracyjnych i test udziału.

Szczegółowe adresacje IP, nazwy urządzeń, konfiguracja VLAN, polityki bezpieczeństwa, harmonogramy kopii zapasowych oraz docelowe reguły UTM powinny zostać ustalone z Zamawiającym przed uruchomieniem produkcyjnym. Wykonawca ma obowiązek zachować poufność wszelkich informacji o środowisku teleinformatycznym Zamawiającego.

Wymagania dotyczące gwarancji i serwisu

Wszystkie dostarczone urządzenia muszą być objęte gwarancją zgodną co najmniej z wymaganiami określonymi przy poszczególnych kategoriach. Gwarancja musi obejmować wady materiałowe, produkcyjne oraz nieprawidłowe działanie sprzętu niewynikające z winy Zamawiającego. W okresie gwarancji Wykonawca zapewni możliwość zgłaszania awarii w dni robocze, a dla urządzeń krytycznych, takich jak serwery i UTM, zgodnie z poziomem wsparcia producenta.

- Bieg gwarancji rozpoczyna się od dnia podpisania protokołu odbioru końcowego bez zastrzeżeń.
- Wykonawca przekaże Zamawiającemu dane kontaktowe do zgłoszeń serwisowych oraz procedurę rejestracji awarii.
- W przypadku wymiany urządzenia lub podzespołu na nowy, wymieniony element musi być wolny od wad i posiadać parametry nie gorsze od elementu pierwotnego.
- Jeżeli nośnik danych zawiera dane Zamawiającego, jego wymiana lub zwrot musi być realizowana zgodnie z zasadami ochrony informacji. Zamawiający może wymagać pozostawienia uszkodzonych nośników danych u siebie, jeżeli wynika to z polityki bezpieczeństwa.
- Aktualizacje firmware i oprogramowania układowego powinny być dostępne co najmniej przez okres gwarancji lub subskrypcji wymaganej dla danego urządzenia.

Wymagania dotyczące dokumentacji

Wykonawca przekaże Zamawiającemu dokumentację umożliwiającą identyfikację, eksploatację, serwisowanie i zarządzanie dostarczonym sprzętem. Dokumentacja może zostać przekazana w formie papierowej lub elektronicznej, z zastrzeżeniem, że dane dostępowe, hasła i klucze licencyjne muszą zostać przekazane w sposób bezpieczny.

- wykaz dostarczonego sprzętu z nazwą producenta, modelem, numerem seryjnym i okresem gwarancji;
- karty katalogowe lub dokumenty producenta potwierdzające spełnienie istotnych parametrów technicznych;
- instrukcje obsługi, montażu i administracji;
- dokumenty licencyjne, numery subskrypcji, potwierdzenia rejestracji lub aktywacji usług;
- protokoły wykonanych czynności instalacyjnych i testowych;
- informacje o sposobie zgłaszania awarii i korzystania z gwarancji.

Wymagania dotyczące odbioru

Odbiór przedmiotu zamówienia nastąpi na podstawie protokołu odbioru podpisanego przez przedstawicieli Zamawiającego i Wykonawcy. Podpisanie protokołu odbioru jest możliwe po potwierdzeniu kompletności dostawy, zgodności dostarczonych urządzeń z OPZ, poprawności podstawowego uruchomienia oraz przekazania wymaganej dokumentacji.

Element odbioru	Sposób weryfikacji
Kompletność dostawy	Porównanie dostarczonych urządzeń, akcesoriów i licencji z OPZ, ofertą oraz dokumentami dostawy.
Zgodność techniczna	Weryfikacja modeli, parametrów, numerów seryjnych, wyposażenia, dokumentacji producenta i informacji licencyjnych.
Stan fizyczny	Kontrola braku widocznych uszkodzeń, kompletności opakowań oraz stanu elementów montażowych.
Uruchomienie	Podstawowy test włączenia, dostępności interfejsów, stanu dysków, baterii, portów i usług zarządzających.
Dokumentacja	Sprawdzenie przekazania instrukcji, kart gwarancyjnych, danych serwisowych, licencji i protokołów wdrożeniowych.

W przypadku stwierdzenia braków, wad lub niezgodności Zamawiający może odmówić odbioru całości lub części dostawy do czasu usunięcia nieprawidłowości przez Wykonawcę. Usunięcie nieprawidłowości następuje na koszt i ryzyko Wykonawcy.

Warunki równoważności

Zamawiający dopuszcza rozwiązania równoważne, o ile spełniają one wszystkie wymagania minimalne określone w OPZ, zapewniają nie gorszą funkcjonalność, wydajność, kompatybilność, bezpieczeństwo, niezawodność i zakres wsparcia niż wymagany. Ciężar wykazania równoważności spoczywa na Wykonawcy.

- Równoważność musi być potwierdzona dokumentacją producenta, kartami katalogowymi, oświadczeniem producenta lub innymi wiarygodnymi dokumentami technicznymi.
- Parametry wyższe od wymaganych są dopuszczalne i nie wymagają odrębnej zgody Zamawiającego, o ile nie powodują ograniczenia funkcjonalności lub kompatybilności.
- Nie uznaje się za równoważne rozwiązania, które wymagają zakupu dodatkowych licencji, modułów lub usług po stronie Zamawiającego, jeżeli elementy te są konieczne do spełnienia OPZ, a nie zostały ujęte w ofercie.
- W przypadku rozwiązań licencjonowanych Wykonawca musi zapewnić legalność korzystania przez Zamawiającego przez cały wymagany okres.

Postanowienia końcowe

Wykonawca, składając ofertę, potwierdza, że zaoferowany sprzęt spełnia wymagania niniejszego OPZ oraz że cena oferty obejmuje wszystkie koszty niezbędne do prawidłowej realizacji zamówienia, w tym koszty dostawy, transportu, wniesienia, akcesoriów, licencji, gwarancji, dokumentacji oraz czynności instalacyjno-uruchomieniowych wskazanych w OPZ.

Wszelkie niejasności dotyczące parametrów technicznych, zakresu dostawy lub sposobu wdrożenia powinny zostać wyjaśnione na etapie postępowania. Po zawarciu umowy Wykonawca nie może powoływać się na brak wiedzy o wymaganiach, jeżeli wynikają one z OPZ, SWZ, odpowiedzi Zamawiającego na pytania wykonawców lub z charakteru kompletnej dostawy sprzętu IT.

Dokument należy traktować jako techniczny załącznik do dokumentacji postępowania. Postanowienia dotyczące kar umownych, terminów płatności, zabezpieczenia należytego wykonania umowy, ochrony danych, poufności oraz zasad zmian umowy powinny zostać określone w SWZ i projekcie umowy.