Numer sprawy: **ZP-ROO.271.1.1014987.2024** Kcynia, dnia 21 listopada 2024 r.

Gmina Kcynia
ul. Rynek 23
89-240 Kcynia

Szczegółowy Opis Przedmiotu Zamówienia

na dostawę sprzętu informatycznego i oprogramowania związaną z realizacją projektu

w ramach grantu Cyberbezpieczny Samorząd

Spis treści

1. Zestawienie ilościowe.

Lp.	Nazwa	Ilość
1.	Zakup serwera	3 szt.
2.	Zakup macierzy dyskowej	1 szt.
3.	Zakup oprogramowania do zarządzania infrastrukturą IT	1 szt.
4.	Zakup systemu backup	1 szt.
5.	Zakup dysków zewnętrznych do backupu	14 szt.
6.	Zakup kluczy sprzętowych	130 szt.

2. Wymagania ogólne w zakresie dostawy sprzętu i oprogramowania.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale", „end-of-support", „end-of-life" producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do każdej wskazanej przez Zamawiającego lokalizacji.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. W ramach prac konfiguracyjnych serwerów i macierzy dyskowej Zamawiający oczekuje stworzenia klastra HA serwerów i macierzy, w tym minimum wymaga: zaprojektowania schematu logicznego LAN dla dostarczanej infrastruktury wraz z uwzględnieniem istniejącej infrastruktury; opracowania założeń optymalizacji ruchu i zapewnienia bezpieczeństwa implementacji i separacji sieci; instalacji urządzeń w szafie RACK; podłączenia urządzeń kablami zasilającymi do gniazd UPS, połączenia dostarczanej infrastruktury ze sobą przy wykorzystaniu portów SFP28 za pomocą kabli światłowodowych i wkładek SFP+, wykonania aktualizacji oprogramowania i firmware'ów na urządzeniach; skonfigurowania połączeń sieciowych na urządzeniach zgodnie z wcześniej zaprojektowanym

schematem logicznym; przeprowadzenie konfiguracji i udostępnienia zasobów dyskowych macierzy dyskowej; migracja maszyn wirtualnych, wykonanie testów akceptacyjnych polegających na weryfikacji poprawności pracy dostarczonych urządzeń; opracowanie i przekazanie Zamawiającemu dokumentacji powykonawczej zainstalowanych urządzeń oraz wykonanych prac instalacyjno-konfiguracyjnych.

11. W ramach zamówienia Wykonawca jest zobowiązany do dostarczenia urządzeń i oprogramowania oraz konfiguracji klastra HA w zakresie oprogramowania dla trzech serwerów serwerowego systemu operacyjnego Microsoft Windows Serwer 2022 Standard lub równoważnego zgodnie z kryteriami równoważności określonymi poniżej dla każdego serwera wraz z licencjami dostępowymi umożliwiającymi korzystanie z zasobów klastra dla 70 użytkowników.
12. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
13. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio uproducenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
14. Wykonawca jest zobowiązany do zachowania w ścisłej poufności wszelkich informacji udostępnionych przez Zamawiającego, które nie zostały przez Zamawiającego ujawnione publicznie.
15. Wykonawca jest zobowiązany wykorzystywać wszelkie informacje poufne wyłącznie w celach wynikających wprost z potrzeby realizacji zamówienia, jedynie w zakresie niezbędnym do jego realizacji.
16. Wykonawca jest zobowiązany nie przekazywać ani nie ujawniać tak informacji poufnych jak i ich źródła osobom trzecim, bez każdorazowej uprzedniej pisemnej zgody Zamawiającego.
17. Wykonawca jest zobowiązany poinformować niezwłocznie Zamawiającego w przypadku, gdy powezmie wiadomość lub podejrzenie naruszenia któregokolwiek ze swoich zobowiązań.
18. Wykonawca jest zobowiązany po zakończeniu lub zaprzestaniu realizacji zamówienia, jak i na każde żądanie Zamawiającego bezzwłocznie zwrócić Zamawiającemu wszelkie materiały udostępnione przez Zamawiającego zawierające informacje poufne i wszystkie ich kopie oraz zniszczy lub usunie wszelkie informacje poufne zapisane w jakimkolwiek urządzeniu lub na jakimkolwiek nośniku służącym do przechowywania danych, w sposób uniemożliwiający ich ponowne odtworzenie.

3. Proces współpracy uruchomienia klastra HA i systemu backup.

1. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uruchomienia produkcyjnego klastra HA oraz migracji maszyn wirtualnych i fizycznych

uwzględniając obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. Wykonawca jest zobowiązany wykonać migrację danych oraz migrację Active Directory z istniejącego serwera w wersji Microsoft Windows 2016 Standard do nowego zaoferowanego w ramach postępowania serwerowego systemu operacyjnego. W projekcie technicznym muszą być zawarte:

a. opis koncepcji realizacji prac przy wykorzystaniu dostarczonego oprogramowania i sprzętu, w tym minimum: opis konfiguracji serwerów i macierzy SAN (utworzenie LUN, zapewnienie Multipathing, utworzenie zasobów współdzielonych), opis migracji maszyn wirtualnych w zakresie wskazanym przez Zamawiającego, opis koncepcji realizacji systemu backup,
b. scenariusze testowe, procedury oraz wzory raportów testów,
c. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
d. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.

2. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
    a. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 30 dni kalendarzowych od dnia zawarcia umowy,
    b. Zamawiający w terminie nie dłuższym niż 7 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
    c. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
    d. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
    e. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
    f. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików z możliwością edycji w standardzie pakietu MS Office lub OpenOffice oraz plików nieedytowalnych gotowych do wydruku, np. w formacie PDF.
3. Wykonawca zrealizuje wdrożenie klastra HA i systemu backup, wykona migracje maszyn wirtualnych i fizycznych zgodnie z zakresem prac i projektem technicznym.
4. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań. Wykonawca opracuje koncepcję backupu dla wdrożonej infrastruktury opierając się na będącym częścią infrastruktury sprzętowo-systemowej Zamawiającego systemie backup oraz dostarczanym systemie backup.
5. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.

6. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery". Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
7. Wykonawca jest zobowiązany przed przystąpieniem do przygotowania projektu technicznego wykonać samodzielną analizę w siedzibie Zamawiającego w zakresie funkcjonujących rozwiązań technicznych w taki sposób aby uwzględnić całość środowiska informatycznego, a wdrażane rozwiązania nie zakłóciły bieżącej pracy istniejących systemów.

Instruktaże.

1. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
2. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
3. Instruktaże powinny trwać minimum 16 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 4 osoby).
4. Zamawiający nie dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
5. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne związane z obsługą, utrzymaniem i monitoringiem klastra HA i systemu backup, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.

4. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie

normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.

5. Brak określenia „minimum" oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich 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.
10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich 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.

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

5. Zakup serwera (3 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2. Płyta główna z możliwością zainstalowania jednego procesora.
3. Zainstalowany jeden procesor klasy x86 dedykowany do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 245 punktów w teście SPECrate2017_fp_base dla konfiguracji jednoprocesorowej według wyników publikowanych na stronie www.spec.org. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 256 GB w najnowszej technologii oferowanej przez producenta, płyta główna musi obsługiwać do min. 1 TB pamięci RAM DDR5.

5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC.
6. Zintegrowana karta graficzna ze złączem VGA.
7. Interfejsy sieciowe: Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25GbE Ethernet w standardzie SFP28 realizowane w oparciu o dwie niezależne karty sieciowe. Wykonawca jest zobowiązany dostarczyć dedykowane wkładki i okablowanie do podłączenia serwerów i macierzy w klaster HA.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 4 dyski twarde Hot-Plug SSD SAS o prędkości min. 24 Gb/s o pojemności co najmniej 1,92 TB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Możliwość zainstalowania co najmniej dwóch dysków M.2 SATA z możliwością konfiguracji RAID 1.
10. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w co najmniej dwa nośniki typu flash z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
11. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
12. Wsparcie dla dysków samoszyfrujących.
13. Wbudowane porty: min. 3 porty USB, w tym co najmniej 1 port USB musi być dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
14. Wentylatory: Redundantne typu Hot Plug.
15. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 1100 W każdy.
16. Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
    2) zdalne monitorowanie i informowanie o statusie serwera,
    3) szyfrowane połączenie oraz autentykacje i autoryzację użytkownika,
    4) możliwość podmontowania zdalnych wirtualnych napędów,
    5) wirtualną konsolę z dostępem do myszy, klawiatury,
    6) wsparcie dla IPv6,
    7) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
    8) integracja z Active Directory,
    9) wsparcie dla dynamic DNS.
17. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
    1) wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
    2) blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
    3) moduł TPM 2.0;
    4) możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera;
    5) możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.

18. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard 2022 wraz z 70 licencjami dostępowymi umożliwiającymi korzystanie przez 70 użytkowników lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.
    Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Standard 2022 wraz z 70 licencjami dostępowymi Microsoft Windows Server 2022 CAL User:
    1) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego dla minimum 70 użytkowników.
    2) Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
    3) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
    4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
    5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
    6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
    7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
    8) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
    9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
    10) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
    11) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
    12) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
    13) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
    14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
    15) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
    16) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
    17) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
    18) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
    19) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
    20) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

19. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
20. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych; Certyfikat NIST SP 800-193 lub inny równoważny dokument potwierdzający, że serwer spełnia wymagania normy NIST SP 800-193 ochrony przed cyberatakami. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów w zakresie określonym powyżej.
21. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia.

6. Zakup macierzy dyskowej (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa typu RACK o wysokości maksymalnie 3U z możliwością instalacji do 24 dysków 2.5" Hot-Plug.
2. Macierz musi posiadać co najmniej 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
3. Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
   Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" i 3,5".

4. Macierz musi posiadać co najmniej 8 portów SFP28 25Gb/s.
5. Zainstalowane min. 12 dysków Hot-Plug SAS SSD min. 24Gb/s o pojemności co najmniej 1,92TB każdy.
6. Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).
7. Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.
8. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).
9. Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
10. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).
11. Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.
12. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
13. Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.
14. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.
15. Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na co najmniej 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
16. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).
17. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, VMWare. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do prze-

łączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.

18. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
19. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje Wykonawca jest je zobowiązany dostarczyć w ramach niniejszego postępowania.
20. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent macierzy opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub inny równoważny dokument poświadczający, że producent macierzy posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowana macierz spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta macierzy lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowaną macierz i jego/ich producenta/producentów w zakresie określonym powyżej.
21. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty macierzy wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej macierzy, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta macierzy. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia.

7. Zakup oprogramowania do zarządzania infrastrukturą IT (1 szt.).

1. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
   a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku jeżeli dostarczone oprogramowanie działa częściowo w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.
   b. Zamawiający wymaga dostarczenia licencji umożliwiającej działanie na co najmniej 100 środowiskach końcowych (stacje robocze, serwery, maszyny wirtualne).

c. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
d. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
e. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
f. Usługa wsparcia wdrożenia obejmuje:
    i. przeprowadzenie analizy przedwdrożeniowej,
    ii. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
    iii. rejestracja produktu – jeżeli wymagana,
    iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
    v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
    vi. konfigurację oprogramowania,
    vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
    viii. szkolenie administratorów z zakresu pracy z programem,
    ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połącznie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.

2. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
    a. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
        i. scenariusze testowe, procedury oraz wzory raportów testów,
        ii. szczegółowy harmonogram realizacji prac wdrożeniowych uwzględniający specyfikę organizacji Zamawiającego,
        iii. opis koncepcji realizacji prac,
        iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
    b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
        i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 30 dni kalendarzowych od dnia zawarcia umowy,
        ii. Zamawiający w terminie nie dłuższym niż 7 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
        iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
        iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,

v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
vi. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.

c. Wykonawca zrealizuje wdrożenia zgodnie z zakresem prac i projektem technicznym.
d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery". Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.

3. Instruktaże w zakresie dostarczonego oprogramowania – wymagania minimalne.
   a. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
   b. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
   c. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 4 osoby).
   d. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
   e. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.
4. Wymagania licencyjne dla dostarczonego oprogramowania:
   a. Licencjobiorcą wszystkich licencji będzie Gmina Kcynia.
   b. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.
   c. Licencje muszą obowiązywać do dnia 20.06.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania.
   d. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
   e. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.

f. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
g. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
h. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
i. Licencja oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.
j. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.

5. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania:
    a. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 20.06.2026 r.
    b. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
    c. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 20.06.2026 r.
    d. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
        i. dostęp do najnowszych wersji oprogramowania,
        ii. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
        iii. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
        iv. przyjmowanie i realizacja zgłoszeń serwisowych,
        v. doradztwo techniczne w zakresie konfiguracji i optymalizacji oprogramowania,

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

6. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi", „powinien", „możliwość" określając w ten sposób wymaganą funkcjonalność oprogramowania.
7. Wykonawca jest zobowiązany przed przystąpieniem do przygotowania projektu technicznego wykonać samodzielną analizę w siedzibie Zamawiającego w zakresie funkcjonujących rozwiązań technicznych w taki sposób aby uwzględnić całość środowiska informatycznego, a wdrażane rozwiązania nie zakłóciły bieżącej pracy istniejących systemów.

Minimalne wymagania funkcjonalne dla oprogramowania specjalistycznego do zarządzania bezpieczeństwem IT:

1. Oprogramowanie musi składać się serwera zarządzającego, zdalnych konsoli oraz Agentów.
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2.

3. Oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.
4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów - nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników.
5. Oprogramowanie musi posiadać funkcjonalność monitorowania infrastruktury serwerowej i sieciowej w zakresie:
   a. wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
   b. wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
   c. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
   d. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
   e. serwerów pocztowych: - monitorowanie serwisu odbierającego, jak i wysyłającego pocztę, - możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), - możliwość wykonywania operacji testowych, - możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa,
   f. monitorowania serwerów WWW i adresów URL,
   g. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
   h. obsługi komunikatów syslog i pułapek SNMP.
   i. monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych- ruchu generowanego przez podłączone stacje robocze,
   j. kontroli nad monitorem usług Windows,
   k. monitorowania wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
6. Oprogramowanie musi umożliwiać automatyczne gromadzenie danych o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie:
   a. informacji dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.;
   b. zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;
   c. informacji o zainstalowanych aplikacjach oraz aktualizacjach Windows, umożliwiających audytowanie i weryfikację użytkowania licencji w organizacji;
   d. informacji o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.;
   e. możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera;
   f. możliwość odczytania numeru seryjnego (klucze licencyjne);
   g. możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;
   h. możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
7. Oprogramowanie musi mieć możliwość prowadzenia bazy ewidencji majątku IT w zakresie:

a. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
b. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz, możliwość importu danych z zewnętrznego źródła np. (.CSV);
c. generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania;
d. archiwizacji i porównywania audytów środków trwałych;
e. tworzenia kodów kreskowych w Środkach Trwałych;
f. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy;
g. inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej co najmniej na system Android;
h. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji dodatkowego oprogramowania poprzez manualne wykonanie skanów inwentaryzacji offline).

8. Oprogramowanie musi zapewniać funkcjonalność w zakresie monitorowania aktywności użytkowników na stacjach roboczych w zakresie:
   a. faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy);
   b. monitorowania procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika);
   c. użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona);
   d. informacji o edytowanych przez użytkownika dokumentach;
   e. historii pracy (cykliczne zrzuty ekranowe);
   f. listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
   g. transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
   h. wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek.
9. Oprogramowanie musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
   a. skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie, archiwów ZIP;
   b. zarządzanie posiadanymi licencjami;
   c. audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji;
   d. zarządzanie posiadanymi licencjami: raport zgodności licencji;

e. możliwość przypisania do programów numerów seryjnych, wartości itp.

10. Oprogramowanie musi zapewniać integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
11. W zakresie pomocy technicznej system musi umożliwiać:
    a. tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów);
    b. załączanie komentarzy, zrzutów ekranów i załączników w zgłoszeniach;
    c. konfigurowanie pól niestandardowych, powiązanych w wybraną kategorią zgłoszenia;
    d. planowanie zastępstw w przydzielaniu zgłoszeń;
    e. funkcję rozbudowanych raportów;
    f. powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym;
    g. baza zgłoszeń z rozbudowaną wyszukiwarką;
    h. przejrzysty i intuicyjny interfejs webowy;
    i. wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych;
    j. komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu;
    k. zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury;
    l. dwukierunkowa wymiana plików;
    m. zarządzanie procesami Windows z poziomu okna informacji o urządzeniu;
    n. zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania);
    o. procesowanie zgłoszeń z wiadomości e-mail;
    p. integracja bazy użytkowników z Active Directory;
    q. zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).
12. W zakresie kontroli dostępu do danych system musi umożliwiać:
    a. automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa;
    b. ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych;
    c. zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych;
    d. integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania;
    e. integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych;
    f. możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB);
    g. alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”);
    h. integracja z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów
    i. zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami;
    j. informacje o urządzeniach podłączonych do danego komputera;
    k. lista wszystkich urządzeń podłączonych do komputerów w sieci;
    l. audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych;
    m. zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników;

n. centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory.

8. Zakup systemu backup (1 szt.).

Przedmiotem zamówienia jest dostawa systemu backup w postaci urządzenia typu all-in-one umożliwiającego:

1. Tworzenie pełnych, przyrostowych i różnicowych kopii zapasowych danych.
2. Automatyczne tworzenie kopii zapasowych zgodnie z harmonogramem.
3. Możliwość przywracania danych na poziomie plików, folderów oraz pełnych systemów.
4. Ochronę przed ransomware poprzez monitorowanie systemu oraz funkcję natychmiastowego przywracania danych.
5. Obsługę deduplikacji danych w celu optymalizacji wykorzystania przestrzeni dyskowej.
6. Zapewnienie wysokiej dostępności danych poprzez replikację.

Minimalne parametry techniczne systemu backup:

1. Obudowa typu RACK wraz z szynami umożliwiającymi montaż urządzenia w szafie RACK.
2. Urządzenie musi oferować przestrzeń min. 24 TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji.
3. Urządzenie musi posiadać minimum 2 porty RJ45 1GbE oraz 2 porty SFP+ 10GbE.
4. Urządzenie musi zapewniać wsparcie dla protokołów CIFS i NFS oraz deduplikacji na źródle.
5. Urządzenie musi zapewniać wsparcie dla systemów operacyjnych: min. Windows, Linux, macOS.
6. Urządzenie musi zapewniać zgodność z systemami plików: NTFS, FAT32, ext3, ext4, XFS.
7. Urządzenie musi zawierać mechanizmy integracyjne z systemami wirtualizacji (min. VMware, Hyper-V) w celu ochrony maszyn wirtualnych.
8. Dostarczone urządzenie musi umożliwiać dodatkową rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention). Urządzenie powinno obsługiwać integrację z chmurami takimi jak AWS, Azure, i Google Cloud.
9. Urządzenie powinno realizować deduplikację in-line oraz kompresję danych przed ich zapisem.
10. Urządzenie powinno być zarządzane przez GUI oraz CLI.
11. Urządzenie powinno wspierać RAID5.
12. Urządzenie powinno oferować funkcjonalność WORM.
13. Urządzenie powinno oferować funkcje typowe dla systemu Disaster Recovery i Business Continuity (BCDR).
14. Urządzenie powinno umożliwiać weryfikację danych oraz zautomatyzowane procesy usuwania przeterminowanych danych.
15. Urządzenie powinno obsługiwać replikację i możliwość podziału na logiczne części.
16. Urządzenie powinno posiadać możliwość skonfigurowania harmonogramu kopii zapasowych opartego na najlepszych praktykach (np. kopia pełna raz w tygodniu, przyrostowa codziennie).
17. Urządzenie powinno zapewniać przepustowość sieciową i wydajność urządzenia dostosowaną do obsługi środowiska bez negatywnego wpływu na codzienną pracę.
18. Urządzenie musi zapewniać szyfrowanie danych zarówno podczas tworzenia kopii zapasowych, jak i podczas ich przesyłania oraz przechowywania (AES-256).
19. Urządzenie musi zapewniać dwustopniową weryfikację dostępu do urządzenia i oprogramowania w celu dodatkowego zabezpieczenia.

20. Urządzenie musi być zgodne z wymogami RODO zapewniając odpowiednie zabezpieczenia danych osobowych oraz możliwość zarządzania danymi zgodnie z prawem.
21. Urządzenie powinno umożliwiać tworzenie, zarządzanie i odzyskiwanie kopii migawkowych.
22. Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway.
23. Wykonawca jest zobowiązany do instalacji i wdrożenia urządzenia w oparciu o wcześniej przygotowany projekt techniczny określony w rozdziale „Proces współpracy uruchomienia klastra HA i systemu backup."
24. Wykonawca zapewni gwarancję urządzenia w okresie 24 miesięcy oraz zapewni wsparcie producenta w okresie do dnia 20.06.2026 r. obejmujące gwarancję aktualizacji oprogramowania do najnowszej wersji.

9. Zakup dysków zewnętrznych do backupu (14 szt.).

Minimalne parametry techniczne dysków zewnętrznych:

1. Typ dysku: zewnętrzny, SSD.
2. Pojemność dysku: min. 2 TB.
3. Prędkość odczytu i zapisu: min. 1000 MB/s.
4. Sprzętowe szyfrowanie: 256-bitowe szyfrowanie danych AES.
5. Interfejs: USB 3.2 Gen. 2, typ C.
6. Odporność na wibracje i upadki.
7. Spełnienie wymagań normy IP65.
8. Oprogramowanie do zarządzania umożliwiające weryfikację stanu urządzenia, optymalizację jego wydajności, definiowanie zabezpieczeń danych.
9. W zestawie kabel do podłączenia Kabel USB-C, z przejściówką na USB-A.
10. Gwarancja producenta: min. 36 miesięcy gwarancji. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia.

10. Zakup kluczy sprzętowych (130 szt.).

Minimalne parametry kluczy sprzętowych:

1. Komunikacja: USB, NFC.
2. Szyfrowanie: RSA 40965, RSA 30725, RSA 2048, RSA 1024, ECC p2566, ECC p3846.
3. Autoryzacja za pomocą protokołu FIDO/FIDO 2.0 w aplikacjach i serwisach internetowych.
4. Autoryzacja za pomocą metody Challenge-Response (np. menedżer haseł KeePassXC).
5. Przechowywanie certyfikatu PIV (logowanie do Active Directory, autoryzacja połączeń SSH).
6. Logowanie użytkownika do systemów operacyjnych Windows, Linux, Mac.
7. Dwuskładnikowe uwierzytelnianie.
8. Przechowywanie klucza OpenPGP do szyfrowania i podpisywania maili, plików.
9. Emulacja SmartCard.
10. Nie może wymagać zasilania z baterii ani połączenia sieciowego do działania.
11. Wykorzystywanie jako tag NFC (np. uruchamianie innych urządzeń, kontrola dostępu).
12. Gwarancja: 24 miesiące gwarancji producenta. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia.