Załącznik Nr 3
do Zapytania ofertowego

Szczegółowy Opis Przedmiotu Zamówienia

na dostawę sprzętu i oprogramowania dla Gminy Kluczewsko w ramach realizacji projektu grantowego „Cyfrowa Gmina”

Spis treści

1. Zestawienie ilościowe.

Lp.	Nazwa	Ilość
1.	Dostawa serwera	1 szt.
2.	Dostawa przełączników sieciowych	4 szt.
3.	Dostawa UPS	1 szt.
4.	Dostawa NAS	1 szt.
5.	Dostawa oprogramowania serwerowego	1 szt.
6.	Dostawa szafy RACK	1 szt.
7.	Zakup usług wdrożenia usług katalogowych	1 szt.
8.	Dostawa oprogramowania specjalistycznego do zarządzania IT	1 szt.
9.	Dostawa oprogramowania specjalistycznego do szyfrowania danych	1 szt.
10.	Dostawa subskrypcji urządzenia UTM	1 szt.

2. Przedmiot zamówienia.

2.1. Wymagania ogólne w zakresie dostawy sprzętu.

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
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” oraz „end-of-support” 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 wskazanej lokalizacji w siedzibie Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzenia 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. 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.

2.2. Zasada równoważności rozwiązań.

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, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
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. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić na komputerze o 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. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić na komputerze o 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.

2.3. Dostawa serwera (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa RACK o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 2.5 cala lub min. 4 dysków 3.5 cala wraz z kompletem wysuwanych szyn wraz z organizerem okablowania umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych.

2. Płyta główna z możliwością zainstalowania dwóch procesorów.

3. Zainstalowane dwa procesory dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 140 punktów w teście SPECrate®2017_fp_base organizacji Standard Performance Evaluation Corporation (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: min. 64 GB w najnowszej technologii producenta, minimum 10 wolnych slotów pamięci.

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.

6. Gniazda PCI: min. dwa sloty PCIe min. Gen 4.

7. Interfejsy sieciowe: minimum 2 porty typu Gigabit Ethernet Base-T, minimum 2 porty typu SFP+ 10 GbE z dedykowanymi wkładkami 10GbE SFP+.

8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD.

9. Zainstalowane 4 dyski twarde SATA o pojemności min. 4 TB każdy. Dyski w konstrukcji Hot Plug z prędkością min. 6 Gb/s każdy. W przypadku uszkodzenia dysków w okresie gwarancji Zamawiający wymaga by uszkodzone dyski pozostały jego własnością.

10. Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający min. 2 GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0/1/5/6/10/50/60.

11. Wbudowane porty: min. 2 porty USB, w tym min. jeden na froncie obudowy, 1 port VGA.

12. Dodatkowe karty: zintegrowana karta graficzna.

13. Wbudowany moduł TPM 2.0.

14. Wentylatory: Redundantne typu Hot Plug.

15. Zasilacze: Redundantne typu Hot Plug.

16. Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:

    a. zdalny dostęp do graficznego interfejsu Web karty zarządzającej,

    b. zdalne monitorowanie i informowanie o statusie serwera,

    c. szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika,

    d. możliwość podmontowania zdalnych wirtualnych napędów,

    e. wirtualną konsolę z dostępem do myszy, klawiatury,

    f. wsparcie dla IPv6,

    g. wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,

    h. integracja z Active Directory,

    i. wsparcie dla dynamic DNS.

17. 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.

18. 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. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów w zakresie określonym powyżej.

19. Wykonawca ma obowiązek zainstalować serwer w dostarczanej szafie RACK oraz dokonać uruchomienia serwera zgodnie z wytycznymi Zamawiającego. Czynności te będą wykonywane w porozumieniu z Zamawiającym oraz pod nadzorem Zamawiającego. Urządzenie musi zostać w uzgodnieniu z Zamawiającym: zintegrowane z posiadanym przez Zamawiającego systemem informatycznym, musi zostać wykonana aktualizacja oprogramowania i firmware'ów na urządzeniu, musi zostać wykonana konfiguracja sieci do pracy serwera. Muszą zostać wykonane testy akceptacyjne polegające na weryfikacji poprawności pracy serwera oraz zainstalowanych usług i ich komunikacji z innymi serwerami i systemami. Musi zostać przygotowana dokumentacja powykonawcza zainstalowanego urządzenia oraz wykonanych prac instalacyjno-konfiguracyjnych.

20. Gwarancja: min. 24 miesiące gwarancji producenta z czasem reakcji w miejscu instalacji sprzętu w następny dzień roboczy. Możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną. W okresie gwarancji wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania, bezpłatny dostęp do aktualnych sterowników zainstalowanych w urządzeniach poprzez możliwość pobrania ich z dedykowanej strony internetowej lub poprzez podanie identyfikatora klienta lub numeru seryjnego. Gwarancja musi obejmować usługę pozostawiania u Zamawiającego uszkodzonych dysków w okresie obowiązywania gwarancji bez dodatkowych opłat.

2.4. Dostawa przełączników sieciowych (4 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: przełącznik – min. 24 porty + 4 porty SFP+, zarządzany.
2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).
3. Dostępne interfejsy: min. 24 x 1000Base-T- RJ-45, 4 SFP+.
4. 4 x wkładki SFP+ 10GbE.
5. Standardy komunikacyjne: IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad IEEE 802.3u, 802.3ae, IEEE 802.3x, IEEE 802.1Q.
6. Przepustowość rutowania/przełączania min. 120 Gbps

7. Rozmiar tablicy MAC min. 16 000.
8. Bufor pamięci dla pakietów min. 1,5 MB.
9. 4xkabel DAC/AOC SFP+ 10GbE min. 3 m (kable muszą być dedykowane do dostarczonego urządzenia).
10. Możliwość łączenia urządzeń w stos min. 4.
11. Inne: funkcje QoS, funkcje ACL, routing statyczny IPv4 i IPv6, zdalne zarządzanie przy pomocy przeglądarki web, możliwość pracy w trybie half i full-duplex, obsługa sieci VLAN (min. 100 sieci VLAN).
12. Wykonawca ma obowiązek zainstalować urządzenia w dostarczanej szafie RACK zgodnie z wytycznymi Zamawiającego oraz dokonać uruchomienia urządzeń zgodnie z wytycznymi Zamawiającego. Czynności te będą wykonywane w porozumieniu z Zamawiającym oraz pod nadzorem Zamawiającego. Urządzenia muszą zostać w uzgodnieniu z Zamawiającym: zintegrowane z posiadanym przez Zamawiającego systemem informatycznym, musi zostać wykonana aktualizacja oprogramowania i firmware'ów na urządzeniach, musi zostać wykonana konfiguracja sieci do pracy urządzeń. Muszą zostać wykonane testy akceptacyjne polegające na weryfikacji poprawności pracy urządzeń i ich komunikacji z serwerami i systemami. Musi zostać przygotowana dokumentacja powykonawcza zainstalowanych urządzeń oraz wykonanych prac instalacyjno-konfiguracyjnych.
13. Gwarancja producenta: minimum 24 miesiące gwarancji producenta.

2.5. Dostawa UPS (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: Rack.
2. Moc pozorna: 5000 VA.
3. Moc rzeczywista: 4500 Wat.
4. Architektura UPSa: line-interactive lub online.
5. Liczba i rodzaj gniazdek z utrzymaniem zasilania: 8 x IEC320 C13 (10A).
6. Liczba, typ gniazd wyj. z ochroną antyprzepięciową: 8 x IEC320 C13 (10A).
7. Typ gniazda wejściowego: IEC320 C14 lub IEC C20.
8. Czas podtrzymania dla obciążenia 100%: min. 4 min.
9. Czas podtrzymania przy obciążeniu 50%: min. 10 min.
10. Zimny start.
11. Układ automatycznej regulacji napięcia (AVR).

12. Wyświetlacz LCD.
13. Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia.
14. Wykonawca ma obowiązek zainstalować urządzenie w dostarczanej szafie RACK zgodnie z wytycznymi Zamawiającego oraz dokonać uruchomienia urządzeń zgodnie z wytycznymi Zamawiającego. Czynności te będą wykonywane w porozumieniu z Zamawiającym oraz pod nadzorem Zamawiającego. Urządzenie musi zostać zainstalowane w uzgodnieniu z Zamawiającym: zintegrowane z posiadanym przez Zamawiającego systemem informatycznym, musi zostać wykonana aktualizacja oprogramowania i firmware'ów na urządzeniach, musi zostać wykonana konfiguracja sieci do pracy urządzeń. Muszą zostać wykonane testy akceptacyjne polegające na weryfikacji poprawności pracy urządzeń i ich komunikacji z serwerami i systemami. Musi zostać przygotowana dokumentacja powykonawcza zainstalowanych urządzeń oraz wykonanych prac instalacyjno-konfiguracyjnych.
15. Gwarancja producenta: min. 24 miesiące realizowanej w miejscu instalacji sprzętu obejmującej baterię, z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia.

2.6. Dostawa NAS (1 szt.)

Minimalne parametry techniczne urządzenia:

1. Obudowa do szafy RACK.
2. Procesor wielordzeniowy.
3. Pamięć RAM: min. 8 GB.
4. Funkcje: wsparcie dla wirtualizacji, scentralizowana pamięć masowa na dane, backup, udostępnianie i przywracanie systemu po awarii.
5. Możliwość zainstalowania łącznie 4 dysków, min. SATA 3 - 6 Gb/s.
6. Zainstalowane dyski: min. 4 dysków 16 TB przeznaczonych do pracy z urządzeniami NAS o minimalnej prędkości obrotów 7200 RPM, bufor min. 256 MB, czas pracy MTBF min. 1000000 h.
7. Poziom RAID: 0, 1, 5, 6.
8. Minimalna kompatybilność dysków: 3,5-calowe dyski twarde SATA; 2,5-calowe dyski SSD SATA.
9. Obsługa połączeń 1 GbE (co najmniej dwa porty) oraz 10 GbE RJ45 (co najmniej dwa porty) wraz z 2 wkładkami 10GbE SFP+ oraz niezbędnymi kablami do połączenia.
10. Porty USB: min. 2 x USB 3.0.
11. Szyny do montażu w szafie RACK.
12. Funkcje: zainstalowane na urządzeniu oprogramowanie dedykowane przez producenta urządzenia do tworzenia kopii zapasowych dostępne także przez przeglądarkę www przy

wykorzystaniu bezpiecznego protokołu transmisji danych (co najmniej ssh); obsługa maszyn wirtualnych VMware / Hyper-V; możliwość tworzenia połączeń sieciowych: fail-over, load balancing, agregacji łącza; buforowanie i nadmiarowa alokacja SSD; kopie migawkowe; uwierzytelnienie użytkowników Active Directory.

13. Wykonawca ma obowiązek zainstalować urządzenie we wskazanej przez Zamawiającego szafie RACK oraz dokonać uruchomienia urządzenia zgodnie z wytycznymi Zamawiającego. Czynności te będą wykonywane w porozumieniu z Zamawiającym oraz pod nadzorem Zamawiającego. Urządzenia muszą zostać w uzgodnieniu z Zamawiającym: zintegrowane z posiadanym przez Zamawiającego systemem informatycznym, musi zostać wykonana aktualizacja oprogramowania i firmware'ów na urządzeniu, musi zostać wykonana konfiguracja sieci do pracy urządzenia. Muszą zostać wykonane testy akceptacyjne polegające na weryfikacji poprawności pracy urządzenia i jego komunikacji z serwerami i systemami. Musi zostać przygotowana dokumentacja powykonawcza zainstalowanego urządzenia oraz wykonanych prac instalacyjno-konfiguracyjnych.

14. Gwarancja producenta: min. 24 miesiące gwarancji realizowanej w miejscu instalacji sprzętu, z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia. Gwarancja musi obejmować także dyski. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.

2.7. Dostawa oprogramowania serwerowego (1 szt.).

W ramach zadania Wykonawca jest zobowiązany dostarczyć oprogramowanie serwerowe w zakresie serwerowego systemu operacyjnego z licencjami dostępowymi oraz oprogramowanie wirtualizacyjne.

<u>Wymagania dla serwerowego systemu operacyjnego z licencjami dostępowymi.</u>

Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard 2022 wraz z licencjami dostępowymi dla 20 użytkowników lub równoważnego zgodnie z poniżej określonymi warunkami równoważności.

Warunki równoważności dla dostawy oprogramowania klasy Microsoft Windows Serwer Standard 2022:

1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

2. Możliwość wykorzystania, co najmniej 120 logicznych procesorów oraz co najmniej 2 TB pamięci RAM w środowisku fizycznym.

3. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.

4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.

9. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;

10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.

13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.

17. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

18. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

19. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).

20. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

21. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

22. O ile to konieczne ze względu na licencjonowanie producenta oferowanego serwerowego systemu operacyjnego Zamawiający wymaga dostarczenia licencji dostępowych dla 20 użytkowników.

Wymagania dla oprogramowania wirtualizacyjnego.

1. Warstwa wirtualizacji oprogramowania powinna umożliwiać instalację bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić wymóg obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagany jest wymóg przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
3. Oprogramowanie do wirtualizacji musi zapewnić wymóg skonfigurowania maszyn wirtualnych z możliwością dostępu do min. 4TB pamięci operacyjnej.
4. Oprogramowanie do wirtualizacji musi zapewnić wymóg przydzielenia maszynom wirtualnym do 64 procesorów wirtualnych.
5. Licencja dostarczonego oprogramowania powinna umożliwiać działanie na minimum dwóch serwerach fizycznych.
6. Oprogramowanie do wirtualizacji zapewniać powinno możliwość skonfigurowania maszyn wirtualnych.
7. Oprogramowanie do wirtualizacji zapewniać powinno możliwość stworzenia dysku maszyny wirtualnej.
8. Rozwiązanie powinno umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
9. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
10. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna ma mieć możliwość działania na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna.
11. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH. z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
12. Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej.

13. Oprogramowanie do wirtualizacji powinno zapewniać możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
14. Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
15. Rozwiązanie powinno zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
16. Oprogramowanie do wirtualizacji musi zapewnić wymóg klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
17. Rozwiązanie powinno mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
18. Wykonawca powinien zapewnić możliwość funkcjonowania oprogramowania zgodnie z określonymi wymaganiami w okresie minimum 24 miesięcy. W okresie udzielonej gwarancji Wykonawca jest zobowiązany zapewnić wsparcie producenta oferowanego oprogramowania umożliwiające co najmniej aktualizację oprogramowania do najnowszych wersji.

2.8. Dostawa szafy RACK (1 szt.).

Minimalne parametry techniczne szafy RACK:

1. Rozmiar: między 42 U – 45 U.
2. Wymiary: maks. 800 x 1000mm. (+/- 5 %).
3. Nośność statyczna: min. 1000 kg.
4. Kąt otwarcia drzwi przednich min. 170 stopni.
5. Budowa: drzwi przednie przeszklone z zamkiem, osłony boczne stalowe pełne z zamkiem, drzwi tylne stalowe perforowane z zamkiem, cztery stalowe belki nośne. Elementy metalowe malowane farbą proszkową.
6. Wyposażenie: 2 x listwa zasilająca RACK 1U z min. 9 gniazdami zasilającymi dostosowanymi do oferowanych urządzeń, 2 x półka o regulowanej głębokości w zakresie min. 500-900 mm z blachy stalowej o nośności min. 150 kg, dostosowany do szafy sufitowy panel wentylacyjny panel wentylacyjny wyposażony w cztery wentylatory z łożyskami kulkowymi o wydajności nie mniejszej niż 160 m3/h, 1 x szuflada 2U z zamkiem wysuwana wykonana z blachy, 2x organizer poziomy kabli stalowy 1U.
7. Wykonawca jest zobligowany do montażu szafy RACK w miejscu wskazanym przez Zamawiającego w pomieszczeniu serwerowni w budynku Urzędu Gminy. Montaż będzie polegał co najmniej na: skrętki komputerowe należy wprowadzić do szafy z przepustu; rozszyć skrętkę, podłączyć do patchpaneli; uziemić szafę; podłączyć szafę do wszystkich mediów; zainstalować organizery, półki, inny dostarczany sprzęt umieścić w szafie RACK i podłączyć.
8. Gwarancja: min. 24 miesiące gwarancji producenta.

2.9. Zakup usług wdrożenia usług katalogowych (1 szt.).

Zakres prac.

1. Wykonawca wykona instalację wszystkich zaoferowanych urządzeń szafie RACK w siedzibie Zamawiającego (serwer, NAS, UTM).
2. Wykonawca wykona wszystkie połączenia logiczne LAN oraz dokona konfiguracji dostarczonych urządzeń zgodnie z zaleceniami Zamawiającego.
3. Rozprowadzi okablowanie logiczne LAN oraz kable energetyczne w wewnątrz szafy RACK.
4. Wykonawca przeprowadzi aktualizację oprogramowania układowego (firmware) zaoferowanych urządzeń do najnowszych wersji zgodnie z bieżącymi zaleceniami producenta sprzętu.
5. Wykonawca przeprowadzi konfigurację istniejących urządzeń sieciowych LAN zgodnie z wymaganiami Zamawiającego.
6. Wykonawca jest zobowiązany do wdrożenia oprogramowania serwerowego systemu operacyjnego na serwerze fizycznym Windows Serwer 2022 lub oferowanym oprogramowaniu równoważnym, w tym kontrolera domeny Active Directory.
7. Wymagania dla usługi wdrożenia usługi katalogowej AD Microsoft Windows Server 2022 lub oferowanego oprogramowania równoważnego:
    a. Usługi katalogowe mają pracować w oparciu o protokół LDAP.
    b. Zastosowane rozwiązania techniczne powinny gwarantować wysoką dostępność i niezawodność usług.
    c. Administratorzy systemu powinni mieć możliwość nadzorowania i sprawnego zarządzania całym systemem.
    d. Pojemność systemu docelowego wynosi 25 stacji roboczych i 20 użytkowników.
    e. Na kontrolerze domeny zostaną zainstalowane zabezpieczenia zgodnie ze standardem stosowanym przez Zamawiającego.
8. Wdrożenie usług katalogowych obejmie poniższe funkcjonalności i czynności:
    a. przeniesienie topologii sieci i struktury organizacyjnej urzędu w usługach katalogowych (grupy, VLAN-y);
    b. zdefiniowanie kont użytkowników;
    c. zaimplementowanie struktury katalogowej: komputery i użytkownicy;
    d. utworzenie i konfiguracja zasobów dyskowych dla profili użytkowników oraz pracy w obrębie grup;
    e. wdrożenie mechanizmów zarządzania z poziomu usług katalogowych kluczowymi aplikacjami w sieci urzędu;
    f. określenie polityk bezpieczeństwa na serwerach usług katalogowych (w domenie);

g. opracowanie struktury Grup Zabezpieczeń i ustalenie praw dostępu do zasobów sieciowych;

h. wdrożenie opracowanej struktury Grup Zabezpieczeń (założenie grup i przypisanie im odpowiednich praw dostępu);

i. założenie kont użytkowników wraz z przypisaniem kont do odpowiednich grup zabezpieczeń;

j. przygotowanie procedury podłączania stacji roboczych do domeny usługi katalogowej;

k. przypięcie do domeny minimum 20 stacji lokalnych w różnych VLAN-ach sieci do domeny wraz z migracją danych użytkowników do nowych profili;

l. opracowanie i wdrożenie skryptów logowania użytkowników, uwzględniających ustalone uprawnienia do zasobów sieciowych w tym implementacja polityki haseł i czasu pracy;

m. konfiguracja obiektów Zasad Grup dotyczących automatycznej aktualizacji stacji roboczych; opracowanie i wdrożenie Zasad Grup, dla automatyzacji konfiguracji stacji roboczych oraz profili użytkowników;

n. stworzenie polityk dostępowych w oparciu o grupy użytkowników grupy katalogowej.

9. Wykonawca przeprowadzi instalację i konfigurację oprogramowania do wykonywania backupu i odzyskiwania danych środowiska z wykorzystaniem macierzy NAS.

10. Wykonawca skonfiguruje repozytoria kopii zapasowych na zasobach utworzonych na dedykowanej macierzy NAS i skonfiguruje zadania wykonywania kopii zapasowych zgodnie z wymaganiami Zamawiającego.

<u>Proces współpracy.</u>

1. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne i instalacyjne publikowane przez oferowanego oprogramowania oraz producentów dostarczanych urządzeń, po wykonaniu analizy istniejących u Zamawiającego rozwiązań wraz z koncepcją wdrożenia infrastruktury programowo-sprzętowej oraz aktualizacji serwerowego systemu operacyjnego uwzględniając obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:

   a. scenariusze testowe, procedury oraz wzory raportów testów,

   b. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,

   c. opis koncepcji realizacji prac,

   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 do edycji i PDF.

3. Wykonawca zrealizuje prace zgodnie z zakresem prac i projektem technicznym w siedzibie Zamawiającego. Zamawiający nie dopuszcza prowadzenia prac z wykorzystaniem dostępu zdalnego do infrastruktury Zamawiającego.

4. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań w siedzibie Zamawiającego. Zamawiający nie dopuszcza prowadzenia prac z wykorzystaniem dostępu zdalnego do infrastruktury Zamawiającego.

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.

<u>Instruktaże.</u>

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 2 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, 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.

<u>Gwarancja.</u>

1. Wykonawca udzieli minimum 24 miesięcznej gwarancji na wykonane prace.

2. W ramach udzielonej gwarancji Wykonawca:

    a. zapewni koordynatora obsługi gwarancyjnej, z którym będą prowadzone wszelkie bieżące uzgodnienia w zakresie realizacji napraw gwarancyjnych,

    b. uruchomi kanał kontaktowy w formie elektronicznej przez stronę www lub za pomocą poczty elektronicznej lub telefonicznej, umożlwiający zgłaszanie awarii,

    c. zapewni realizację serwisu gwarancyjnego w języku polskim,

    d. zapewni pomoc w rozwiązywaniu problemów technicznych związanych z funkcjonowaniem rozwiązania powstałego w trakcie realizacji zamówienia,

    e. zapewni obsługę problemów w przypadku ich wystąpienia: usuwanie wad konfiguracyjnych rozwiązania wdrożonego w ramach realizacji zamówienia, przywracanie pełnej funkcjonalności działania wdrożonego rozwiązania, jeżeli jego niewłaściwe działanie bądź awaria wynika z instalacji lub konfiguracji zrealizowanych w ramach zamówienia.

3. Zgłoszenie awarii będzie możliwe przez 7 dni w godzinach 00:00 - 24:00 przez stronę www wskazaną przez Wykonawcę, lub za pomocą poczty elektronicznej na adres wskazany przez Wykonawcę. Przez awarię rozumie się wadę wdrożonego systemu, zdarzenie, w wyniku którego uszkodzeniu uległ jeden (lub więcej) element, ograniczający jego wydajność i funkcjonalność lub uniemożliwiający Zamawiającemu korzystanie z systemu zgodnie z jego Specyfikacją Techniczną/Instrukcją użytkowania lub zmniejszając bezpieczeństwo.

4. Czas reakcji (rozumiany jako maksymalny czas, jaki może upłynąć pomiędzy zgłoszeniem awarii a reakcją Wykonawcy) na podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nie może przekroczyć 24 godzin od momentu gwarancyjnego

zgłoszenia awarii przez Zamawiającego jeżeli do zgłoszenia doszło do godziny 15 w dni robocze z zastrzeżeniem, że reakcja musi nastąpić w następny dzień roboczy.

5. Usunięcie awarii powinno nastąpić w 3 dni robocze od momentu zgłoszenia awarii.
6. Wszelkie koszty związane z naprawami gwarancyjnymi, usuwaniem Awarii, włączając w to koszt podróży z i do siedziby Zamawiającego ponosi Wykonawca.
7. Dopuszcza się po uzgodnieniu z Zamawiającym połączenie zdalne do sieci informatycznej, przez system zdalnego dostępu Zamawiającego, którym zarządzają wyznaczeni administratorzy Zamawiającego.
8. Usunięcie awarii będzie każdorazowo potwierdzone protokołem wykonania naprawy.

2.10. Dostawa oprogramowania specjalistycznego do zarządzania IT (1 szt.).

Minimalne wymagania funkcjonalne dla oprogramowania specjalistycznego do zarządzania siecią i zasobami 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. przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach");

e. dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę;

f. planowanie zastępstw w przydzielaniu zgłoszeń;

g. funkcję rozbudowanych raportów;

h. powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym;

i. baza zgłoszeń z rozbudowaną wyszukiwarką;

j. przejrzysty i intuicyjny interfejs webowy;

k. wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych;

l. komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu;

m. zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury;

n. dwukierunkowa wymiana plików;

o. zarządzanie procesami Windows z poziomu okna informacji o urządzeniu;

p. zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania);

q. procesowanie zgłoszeń z wiadomości e-mail;

r. integracja bazy użytkowników z Active Directory;

s. zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).

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.

<u>Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:</u>

1. Instalacja ma odbyć się na wszystkich komputerach oraz serwerach posiadanych przez Zamawiającego – 20 użytkowników.

2. Zamawiający dopuszcza instalację i wdrożenie zdalne.

3. Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.

4. Usługa wsparcia wdrożenia obejmuje:

    a. analizę przedwdrożeniowa,

    b. pomoc przy instalacji silnika bazy danych - jeżeli będzie wymagana instalacja,

c. instalację oprogramowania: na stacji roboczej,

d. dystrybucję oprogramowania na wybranych stacjach roboczych,

e. konfigurację oprogramowania,

f. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,

g. szkolenie administratorów z zakresu pracy z programem:

h. przykładowy audyt oprogramowania i plików na wybranej stacji roboczej,

i. generowanie raportów i zestawień dotyczących sprzętu, oprogramowania i użytkowników,

j. użytkowanie zdalnego pulpitu.

k. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połącznie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.

<u>Wymagania licencyjne dla dostarczonego oprogramowania:</u>

1. Licencjobiorcą wszystkich licencji będzie Gmina Kluczewsko.
2. Licencje muszą zostać wystawione na czas nieoznaczony (bezterminowy).
3. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
4. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do rozbudowy, zwiększenia ilości serwerów obsługujących oprogramowanie, przeniesienia oprogramowania na inny serwer, rozdzielenia funkcji serwera (osobny serwer bazy danych, osobny serwer aplikacji, osobny serwer plików).
5. Licencja oprogramowania musi być licencją bez ograniczenia ilości komputerów, serwerów, na których można zainstalować i używać oprogramowanie.
6. 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.
7. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
8. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.

9. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).

10. Wykonawca zapewni minimum 24 miesięczną gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.

2.11. Dostawa oprogramowania specjalistycznego do szyfrowania danych (1 szt.).

Oprogramowanie szyfrujące powinno umożliwiać:

1. Szyfrowanie dowolnie wybranych przez użytkownika plików i folderów oraz szyfrowanie całych dysków.

2. Szyfrowanie poczty e-mail i załączników.

3. Szyfrowanie tekstu całych dokumentów lub ich dowolnej części.

4. Tworzenie zaszyfrowanych woluminów oraz archiwów samorozpakowujących.

5. Oprogramowanie powinno posiadać polskojęzyczny interfejs.

6. Oprogramowanie powinno zapewniać standard szyfrowania FIPS 140-2, wykorzystując 256-bitowy algorytm szyfrujący AES.

7. Licencja na oprogramowanie szyfrujące dane powinna umożliwiać pracę minimum 20 użytkownikom i posiadać minimum 12-miesięczne wsparcie producenta.

2.12. Dostawa subskrypcji urządzenia UTM (1 szt.).

Zamawiający przewiduje dostawę subskrypcji do istniejącego urządzenia Stromshield SN300 umożliwiającej działanie następujących funkcji urządzenia w zakresie minimalnym: AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie email na okres do dnia 29.12.2023 r.

W przypadku jeżeli Wykonawca nie może dostarczyć subskrypcji do istniejącego urządzenia Stromshield SN300 Zamawiający dopuszcza możliwość dostarczenia nowego urządzenia wraz z subskrypcją na okres do 29.12.2023 r. jako rozwiązanie równoważne do oczekiwanego. W takim przypadku Wykonawca skonfiguruje urządzenie UTM w zakresie obejmującym minimum: aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta; aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email etc.); konfiguracja routingów statycznych na firewallu, konfiguracja polityki bezpieczeństwa (reguły dostępu dla ruchu z Internetu, do Internetu oraz między pozostałymi strefami) zgodnie z wytycznymi ze strony Zamawiającego; konfiguracja filtracji stron WWW na podstawie kategorii oraz treści; integracja UTM z systemem autoryzacji AD tak aby możliwa była identyfikacja użytkowników; konfiguracja dostępu zdalnego SSL VPN (VPN Client, portal WebVPN);

konfiguracja SSL descryption łącznie z instalacją certyfikatów na stacjach klienckich np. przy użyciu funkcjonalności AD.

Minimalne parametry urządzenia oferowanego jako rozwiązanie równoważne:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym.

System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

Minimalne parametry techniczne urządzenia:

1. Przepustowość Firewall: min. 4 Gbps.
2. Musi obsługiwać min. 300 000 jednoczesnych połączeń.
3. Musi obsługiwać co najmniej 20 jednoczesnych połączeń SSL VPN.
4. Przepustowość IPS: min. 2,4 Gbps.
5. Wydajność SSL VPN: min. 600 Mbps.
6. Automatyczna aktualizacja plików sygnatur antywirusowych.
7. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
8. Automatyczna aktualizacja sygnatur IPS.
9. IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.
10. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
11. Ilość interfejsów sieciowych: minimum 8 portów Gigabit Ethernet RJ-45. Interfejsy te powinny być skonfigurowane jako jeden z trzech rodzajów wymaganych stref bezpieczeństwa.
12. Administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania.

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

    a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

    b. Kontrola Aplikacji.

    c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

    d. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS.

    e. Ochrona przed atakami - Intrusion Prevention System.

    f. Kontrola stron WWW.

    g. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

    h. Zarządzanie pasmem (QoS, Traffic shaping).

    i. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

    j. Analiza ruchu szyfrowanego protokołem SSL.

14. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

15. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.

16. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

17. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

18. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.

19. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

20. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

21. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

22. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
23. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
24. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
25. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
26. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
27. Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
28. Urządzenie powinno mieć możliwość generowania raportów.
29. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
30. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
31. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
32. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
33. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
34. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
35. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres do 29.12.2023 r.
36. Gwarancja producenta min. 12 miesięcy. Gwarancja powinna obejmować również możliwość wymiany urządzenia na nowe w przypadku wady urządzenia UTM.