Numer sprawy: ZP. 271.12.2022

Gorzkowice dnia 23 listopada 2022

Szczegółowy Opis Przedmiotu Zamówienia

na dostawy sprzętu i oprogramowania wraz z przeprowadzeniem szkoleń związane z realizacją projektu w ramach grantu „Cyfrowa Gmina”

Spis treści

1. Zestawienie ilościowe.

Część nr 1 – Dostawa licencji oprogramowania wraz z przeprowadzeniem szkolenia.

Lp.	Nazwa	Ilość
1.	Dostawa licencji oprogramowania do inwentaryzacji sprzętu i oprogramowania	1 szt.
2.	Przeprowadzenie szkolenia w zakresie oprogramowania do inwentaryzacji sprzętu i oprogramowania	1 szt.
3.	Dostawa licencji oprogramowania OCR	1 szt.
4.	Rozbudowa oprogramowania antywirusowego	1 szt.

Część nr 2 – Dostawa sprzętu informatycznego z oprogramowaniem na potrzeby serwerowni.

Lp.	Nazwa	Ilość
1.	Dostawa stacji roboczych	2 szt.
2.	Dostawa skanera	1 szt.
3.	Dostawa urządzenia wielofunkcyjnego	1 szt.
4.	Dostawa kluczy U2F	4 szt.
5.	Dostawa serwera	2 szt.
6.	Dostawa licencji serwerowego systemu operacyjnego (SSO) wraz z licencjami dostępowymi	2 szt.
7.	Dostawa urządzenia NAS wraz z dyskami	1 szt.
8.	Dostawa urządzenia UTM	3 szt.
9.	Dostawa licencji oprogramowania do przechowywania i analizy logów	1 szt.
10.	Przeprowadzenie szkolenia w zakresie SSO i urządzenia UTM	3 szt.

2. Przedmiot zamówienia dla części nr 1.

2.1. 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.

2.2. Dostawa licencji oprogramowania do inwentaryzacji sprzętu i oprogramowania (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.

Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:

1. Instalacja ma odbyć się na wszystkich komputerach oraz serwerach posiadanych przez Zamawiającego – 40 użytkowników.
2. Zamawiający przeprowadzi instalację i wdrożenie oprogramowania we własnym zakresie.
3. Wykonawca będzie udzielał pomocy technicznej Zamawiającemu przez okres gwarancji.

Wymagania licencyjne dla dostarczonego oprogramowania:

1. Licencjobiorcą wszystkich licencji będzie Gmina Gorzkowice.
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 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.
6. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
7. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
8. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).
9. Wykonawca zapewni minimum 12 miesięczną gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.

2.3. Przeprowadzenie szkolenia w zakresie oprogramowania do inwentaryzacji sprzętu i oprogramowania (1 szt.).

Wykonawca musi zapewnić usługę przeprowadzenia autoryzowanego szkolenia certyfikowanego administratora w zakresie oprogramowania do inwentaryzacji sprzętu i oprogramowania. Szkolenie powinno być przeprowadzone w systemie autoryzowanych przez producenta oprogramowania szkoleń. Szkolenie powinno zostać przeprowadzone przez osobę uprawnioną do przeprowadzenia szkolenia zgodnie z wymaganiem szkoleń autoryzowanych producenta oferowanego oprogramowania.

Zakres programowy szkolenia musi wynikać bezpośrednio z autoryzowanego przez producenta oferowanego oprogramowania

Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolona 1 osoba - pracownik Urzędu Gminy Gorzkowice.
2. Szkolenie musi być prowadzone przez instytucję uprawnioną do realizacji szkoleń autoryzowanych i zakończyć się wydaniem certyfikatu Certified Administrator dla oferowanego oprogramowania.
3. Szkolenie może odbywać się poza siedzibą Urzędu, jednak w odległości maksymalnie 200 km od siedziby urzędu. Zamawiający dopuszcza prowadzenie szkolenia w trybie on-line o ile jest to dopuszczone przez autoryzowany przez producenta urządzenia system szkoleń.
4. Szkolenie musi być prowadzone w języku polskim, Zamawiający dopuszcza materiały w języku angielskim.
5. Szkolenie powinno trwać minimum 16 godzin szkoleniowych.

2.4. Dostawa licencji oprogramowania OCR (1 szt.).

Minimalne parametry funkcjonalne oprogramowania:

1. Oprogramowanie powinno umożliwiać przetwarzanie wsadowe dokumentów, indeksowanie oraz automatyczny OCR. Oprogramowanie powinno umożliwiać automatyczną zamianę dokumentów z postaci papierowej oraz ich wprowadzanie do systemu EZD PUW w następującym zakresie:
    a. wspomagania skanowania,
    b. opisu pełno tekstowego OCR, odczytu OMR
    c. automatycznego wprowadzania do systemu obiegu dokumentów.
1. Oprogramowanie powinno zapewniać obsługę wsadów dokumentów, w której dokumenty separowane są kodami kreskowymi (np. drukowanymi na stanowisku przyjmowania dokumentów), kodami typu patch, pustą kartką, ilością skanów oraz separacją po zmianie wartości w polu OCR (indeksie).
2. Oprogramowanie powinno zapewniać możliwość automatycznego OCR i rozpoznawania znaków OMR skanowanych pism bez limitu skanowanych/procesowanych dokumentów.
3. Przez skanowanie rozumie się możliwość odczytania dokumentów z dysku twardego (przetwarzania dokumentów z wybranego folderu) lub skanowania ze skanera dokumentowego.
4. Oprogramowanie na zeskanowanych dokumentach pozwalać powinno na rozpoznawanie i indeksowanie co najmniej 22 typów kodów kreskowych takich typów jak: Aztec, Codebar, Code 39, Code 93, Code 128, Data Matrix, EAN, Interleaved 2 of 5, PDF 417, Post Net, QR, Code 2 of 5, UPC-A, UPC-E.
5. Oprogramowanie na zeskanowanych dokumentach powinno dawać możliwość filtrowania rozpoznawanych kodów do długości, formatów jakie mają spełniać skanowane kody oraz możliwość kontrolowania sumy kontrolnej kodów dla kodów kreskowych obsługujących sumy kontrolne (typy kodów które obsługują sumy kontrolne zapisywane na ostatnich pozycjach to Codebar, Code 39, Interleaved 2 of 5).
6. Oprogramowanie powinno zapewniać rozpoznanie kodu kreskowego na pierwszej stronie również na rewersie dokumentu. W momencie braku takowego na pierwszej stronie odczyt z drugiej lub trzeciej strony powinien być zapewniony.
7. Oprogramowanie powinno pozwalać na zaprogramowanie odpowiednich pól indeksowych, które muszą być rozpoznane w sposób automatyczny oraz umożliwić wprowadzenie wartości indeksu

ręcznie bądź za pomocą metody point&click oraz drag&drop. Każde pole indeksowe musi pozwalać na wybór języka OCR.

8. Oprogramowanie powinno pozwalać na separację zeskanowanych dokumentów na podstawie rozpoznanych i przefiltrowanych kodów obcych zarówno z pierwszej jak i drugiej strony dokumentu wiodącego. W momencie braku takowego na pierwszej stronie odczyt z drugiej lub trzeciej strony będzie zapewniony.
9. Oprogramowanie powinno pozwalać na separację zeskanowanych dokumentów na podstawie pustych stron z możliwością konfiguracji takiego algorytmu rozpoznawania pustych.
10. Oprogramowanie powinno pozwalać na separację zeskanowanych dokumentów na podstawie stałej zadeklarowanej ilości stron na dokument.
11. Oprogramowanie powinno umożliwiać zeskanowanie jednej strony lub całej ilości dokumentów.
12. Oprogramowanie powinno umożliwiać zapis plików na serwerach FTP, SFTP.
13. Oprogramowanie powinno umożliwiać wybór podajnika skanera (ręczny lub automatyczny).
14. Oprogramowanie powinno umożliwiać wybór trybu skanowania (jedno-stronny/dwu-stronny).
15. Oprogramowanie powinno umożliwiać wybór rozmiaru papieru do skanowania oraz wyboru orientacji skanowania (pozioma, pionowa).
16. Oprogramowanie powinno umożliwiać automatyczną rotację skanowanych dokumentów o podstawowe kąty: 90,180,270 stopni. Możliwość definiowania obrotu na każdą stronę oddzielnie.
17. Oprogramowanie powinno umożliwiać doskanowanie dokumentu do całej przetwarzanej grupy.
18. Oprogramowanie powinno umożliwiać podgląd listy zeskanowanych i porozdzielanych dokumentów. Przez widok podziału rozumie się możliwość przejrzenia wszystkich zeskanowanych stron pogrupowane w procesie separacji na dokumenty.
19. Oprogramowanie powinno umożliwiać doskanowanie strony w wybranym miejscu.
20. Oprogramowanie powinno umożliwiać wymianę jednej strony z całego odseparowanego dokumentu.
21. Oprogramowanie powinno umożliwiać przeskanowanie całego wybranego dokumentu, tak aby w przypadku stwierdzenia złego zeskanowania konkretnego dokumentu nie wymagałoby to skanowania całej grupy dokumentów a tylko wymiany tego jednego wadliwego.
22. Oprogramowanie powinno umożliwiać modyfikację dokumentów - przenoszenia stron i dokumentów w obrębie całej grupy zeskanowanych dokumentów.
23. Oprogramowanie powinno umożliwiać automatyczne przełączanie zaprogramowanych zadań lub ustawień skanera za pomocą kodów typu patch umieszczonego pomiędzy skanowanymi dokumentami.
24. Oprogramowanie powinno umożliwiać cofanie wykonywanych operacji.
25. Oprogramowanie powinno umożliwiać przywrócenie pracy nad zeskanowaną grupą dokumentów po zaniku napięcia na stacji skanującej.
26. Oprogramowanie powinno umożliwiać eksport przetworzonych dokumentów do wskazanego folderu. Eksportowane dokumenty powinny mieć możliwość konfiguracji nazewnictwa wykorzystując przy tworzeniu dynamicznych nazw wcześniej rozpoznanych kodów, stałej znakowej, nazwy stacji wykonującej skanowanie, nazwy użytkownika, daty i czasu wykonania operacji. Eksport umożliwiać powinien wyeksportowanie dokumentów w formatach: PDF,PDF-A/1 PDF-A/2 PDF-A/3,PDF-MRC, PDF-BookMark , TIFF,JPG.
27. Oprogramowanie powinno umożliwiać dynamiczny podgląd dokumentów podczas skanowania.
28. Oprogramowanie powinno umożliwiać przetwarzanie dokumentów z folderu takich typów jak TIFF, BMP, JPEG, PDF.
29. Oprogramowanie powinno umożliwiać dla eksportowanych dokumentów PDF ich przeszukiwanie (wyszukiwanie tekstu w dokumentach PDF) oraz zapewnia zabezpieczenie takiego pliku hasłem.

30. Oprogramowanie powinno umożliwiać eksportowanie dokumentów w tle tak aby możliwe było w tym czasie kolejne skanowanie dokumentów.
31. Oprogramowanie powinno umożliwiać walidację rozpoznawanych pól przy użyciu sterowników ODBC które wyszukiwałyby w takiej bazie danych sterownika ODBC rozpoznanego tekstu.
32. Oprogramowanie powinno umożliwiać tworzenie indywidualnego interfejsu użytkownika dla każdej z zalogowanych osób.
33. Oprogramowanie powinno posiadać polski interfejs użytkownika.
34. Oprogramowanie powinno umożliwiać dla funkcji OCR przy indeksowaniu dla każdego z uprzednio definiowanych pól oraz w trybie pełno tekstowym.
35. Oprogramowanie powinno umożliwiać uwierzytelnienie dla użytkowników za pomocą loginu domenowego oraz Active Directory.
36. Wykonawca zapewni gwarancję producenta na oferowane oprogramowanie na okres 24 miesięcy uwzględniającą możliwość aktualizacji do najnowszych wersji oprogramowania.

2.5. Rozbudowa oprogramowania antywirusowego (1 szt.).

UWAGA! TERMIN REALIZACJI ROZBUDOWY OPROGRAMOWANIA ANTYWIRUSOWEGO WYNOSI 5 DNI OD DNIA ZAWARCIA UMOWY.

1. Przedmiotem zamówienia jest aktualizacja oprogramowania - upgrade licencji oprogramowania antywirusowego ESET Endpoint (100 licencji), pozwalający na użytkowanie najnowszej wersji programu ESET PROTECT ENTRY ON – PREM (104 licencji) lub równoważnego systemu antywirusowego zgodnie z poniżej wskazanymi warunkami równoważności.
2. Wykonawca zapewni licencję umożliwiającą działanie całego systemu ESET PROTECT ENTRY ON – PREM rozbudowanego lub równoważnego systemu antywirusowego zgodnie z poniżej wskazanymi warunkami równoważności w ramach niniejszego postępowania do dnia 31 grudnia 2026 r.
3. Licencjobiorcą licencji będzie Gmina Gorzkowice.
4. Oferowana licencja musi pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
5. 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).
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.

Warunki równoważności dla rozwiązania równoważnego do rozbudowy istniejącego oprogramowania antywirusowego:

1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.

2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.
8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
17. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).
18. Rozwiązanie musi wspierać architekturę ARM64.
19. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
20. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
21. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

22. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
23. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
24. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
25. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
26. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
27. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
28. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
29. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
30. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
31. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: „tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, „tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, „tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, „tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, „tryb inteligentny”, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
32. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
33. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
34. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
35. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

36. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
37. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
38. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: „tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, „tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, „tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, „tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
39. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
40. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
41. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
42. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
43. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
44. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2019/2022 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.
45. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
46. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
47. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
48. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
49. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
50. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
51. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
52. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
53. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
54. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
55. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
56. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych

Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

57. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
58. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
59. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
60. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
61. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
62. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
63. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN.
64. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów.
65. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
66. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
67. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
68. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
69. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
70. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.

3. Przedmiot zamówienia dla części nr 2.

3.1. 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 przez Zamawiającego.

7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzenia 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. 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.
11. Dla dostaw sprzętu informatycznego z systemem operacyjnym Zamawiający wymaga fabrycznie nowego systemu operacyjnego (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 systemu operacyjnego nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku systemu operacyjnego 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 u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

3.2. 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.

3.3. Dostawa stacji roboczych (2 szt.).

Minimalne parametry techniczne stacji roboczych:

1. Zestaw komputerowy musi być przeznaczony do zastosowań biurowych.
2. Procesor wielordzeniowy zintegrowany z układem graficznym osiągający w teście wydajności CPU PassMark Performance Test (https://www.cpubenchmark.net) osiągający wynik co najmniej 12 000 punktów zgodnie z wykazem wyników testów wydajności CPU PassMark Performance Test **stanowiącym załącznik nr 1B do SWZ.** Zamawiający żąda załączenia dokumentu potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności do dokumentacji powykonawczej.
3. Pamięć operacyjna min. 16 GB w najnowszej technologii oferowanej przez producenta komputera, przy czym komputer musi posiadać min. 1 niezajęte złącze do rozbudowy i obsługiwać do 32 GB pamięci.
4. Pamięć masowa – dysk w technologii SSD z interfejsem M2 o pojemności min. 500 GB.
5. Karta graficzna zintegrowana z możliwością dynamicznego przydzielania pamięci w obrębie pamięci systemowej.
6. Zintegrowana karta dźwiękowa musi obsługiwać dźwięk 24bit HD.

7. BIOS zgodny ze specyfikacją UEFI.
8. Obudowa musi zapewniać bezpośrednie podłączenie co najmniej dwóch urządzeń USB oraz mikrofonu z przodu oraz łączna suma rozmiarów obudowy (szerokość+wysokość+głębokość) nie może przekraczać 80 cm.
9. Komputer musi być wyposażony w zasilacz wewnętrzny o mocy maksymalnej nieprzekraczającej 250 W.
10. Moduł TPM2.0.
11. Wyposażenie minimalne: nieusuwalne 2xDP lub 2xHDMI (lub mieszane, umożliwiające bezpośrednie podłączenie z monitorem bez stosowania adapterów); nieusuwalne co najmniej 6 portów USB, w tym co najmniej 2 x USB na panelu przednim komputera, napęd optyczny DVD-RW; klawiatura USB w układzie polski programisty i mysz USB (dwuprzyciskowa, rolka/scroll jako trzeci przycisk); 1x wyjście słuchawkowe oraz 1x wejście mikrofonowe na panelu przednim obudowy (dopuszcza się jedno wspólne złącze słuchawkowo – mikrofonowe), karta sieciowa 10/100/1000 Mbit/s Ethernet RJ 45 wspierająca obsługę WoL.
12. Oferowany komputer musi zostać dostarczony z bezterminową licencją oprogramowania systemu operacyjnego klasy Microsoft Windows 11 Professional lub równoważny. Za równoważny system operacyjny Zamawiający uzna system spełniający następujące minimalne parametry: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6; Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe; Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; Wbudowany system pomocy w języku polskim; System operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; System posiadać powinien narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; Graficzne środowisko instalacji i konfiguracji; Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; Możliwość przywracania plików systemowych; Możliwość „downgrade” do niższej wersji.

13. Oferowany komputer musi zostać dostarczony z licencją bezterminową oprogramowania pakietu biurowego klasy Microsoft Office 2021, (licencja przeznaczona dla instytucji rządowych typu government), umożliwiające pracę z edytorem tekstów i arkuszem kalkulacyjnym oraz posiadający narzędzie do przygotowania i prowadzenia prezentacji wraz z narzędziem do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) lub równoważny. Za równoważny system pakietu biurowego Zamawiający uzna system spełniający następujące minimalne parametry:
    a) Dostawa pełnej polskiej wersji językowej interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach pracy Urzędu – cena połączenia nie większa niż cena połączenia lokalnego. Publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej trzech lat od daty zakupu. Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).
    b) Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej:
        - edytor tekstów,
        - arkusz kalkulacyjny,
        - narzędzie do przygotowania i prowadzenia prezentacji,
        - narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).
    c) Edytor tekstów musi umożliwiać co najmniej:
        - Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
        - Wstawianie oraz formatowanie tabel.
        - Wstawianie oraz formatowanie obiektów graficznych.
        - Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
        - Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
        - Automatyczne tworzenie spisów treści.
        - Formatowanie nagłówków i stopek stron.
        - Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
        - Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
        - Określenie układu strony (pionowa/pozioma).
        - Wydruk dokumentów.
        - Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.

- Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
- Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

d) Arkusz kalkulacyjny musi umożliwiać co najmniej:
- Tworzenie raportów tabelarycznych.
- Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
- Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
- Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
- Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.
- Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
- Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
- Wyszukiwanie i zamianę danych.
- Wykonywanie analiz danych przy użyciu formatowania warunkowego.
- Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
- Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
- Formatowanie czasu, daty i wartości finansowych z polskim formatem.
- Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
- Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

e) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać co najmniej:
- Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego.
- Drukowanie w formacie umożliwiającym robienie notatek.
- Zapisanie jako prezentacja tylko do odczytu.
- Nagrywanie narracji i dołączanie jej do prezentacji.
- Opatrywanie slajdów notatkami dla prezentera.
- Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
- Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
- Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
- Możliwość tworzenia animacji obiektów i całych slajdów.
- Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.

f) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

- Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
- Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
- Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
- Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
- Automatyczne grupowanie poczty o tym samym tytule.
- Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
- Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
- Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
- Zarządzanie kalendarzem.
- Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
- Przeglądanie kalendarza innych użytkowników.
- Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
- Zarządzanie listą zadań.
- Zlecanie zadań innym użytkownikom.
- Zarządzanie listą kontaktów.
- Udostępnianie listy kontaktów innym użytkownikom.
- Przeglądanie listy kontaktów innych użytkowników.

14. Każdy komputer musi zostać wyposażony w monitor o parametrach minimalnych:
    a. Typ ekranu: ekran ciekłokrystaliczny LED IPS z matową matrycą min. 23 cali.
    b. Jasność: min. 250 cd/m2.
    c. Kontrast: statyczny min. 1000:1.
    d. Kąty widzenia (pion/poziom): 178 stopni.
    e. Czas reakcji matrycy: maks. 5 ms.
    f. Rozdzielczość ekranu: min. 1920 x 1080 (FullHD).
    g. Format obrazu: 16:9.
    h. Częstotliwość odświeżania ekranu: min. 60 Hz.
    i. Łączność: min. 2 x HDMI (lub 1 x HDMI + 1 x DP umożliwiające bezpośrednie podłączenie z jednostką centralną bez stosowania adapterów), min. 1 x wyjście audio.
    j. Inne: obrotu ekranu; regulacja wysokości, regulacja kąta pochylenia, regulacja kąta obrotu, możliwość montażu na ścianie VESA, możliwość zabezpieczenia linką (Kensington Lock).
15. Dokumenty potwierdzające jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent jednostki centralnej i monitora opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub inny równoważny dokument poświadczający, że producent jednostki centralnej i monitora posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowana jednostka centralna i monitor spełniają 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 jednostki centralnej i monitora lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia dokumentów potwierdzających spełnienie przez oferowaną jednostkę centralną i monitor oraz jego/ich producenta/producentów w zakresie określonym powyżej do dokumentacji powykonawczej.

16. Gwarancja: min. 24 miesiące gwarancji producenta na jednostkę centralną i monitor świadczona na miejscu u użytkownika końcowego. Czas reakcji serwisu - do końca następnego dnia roboczego. Serwis urządzeń musi byś realizowany przez producenta lub autoryzowanego partnera serwisowego producenta. Dostęp do aktualnych sterowników zainstalowanych w komputerze urządzeń, realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego komputera, na dedykowanej przez producenta stronie internetowej umożliwiającej zgłaszanie awarii lub usterek oraz sprawdzenie okresu gwarancji jednostki centralnej i monitora.

3.4. Dostawa skanera (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Rozmiar – A4, skaner z podajnikiem.
2. Kolor: 24-bity, skala szarości: 8-bitów.
3. Rozdzielczość optyczna – min. 600 dpi.
4. Prędkość skanowania – min. 40 str./min.
5. Skan dwustronny.
6. Automatyczny podajnik papieru.
7. Obciążenie dzienne – min. 2000 stron
8. Pojemność podajnika – min. 60 arkuszy A4.
9. Interfejs – min. 1 x USB, karta sieciowa bezprzewodowa WiFi, karta sieciowa LAN RJ45.
10. Zapis do obrazów JPEG, TIFF, PDF, przeszukiwalne pliki PDF.
11. Funkcje dodatkowe: automatyczna orientacja stron, pomijanie pustych stron, wbudowany OCR w języku polskim, rozpoznawanie kodów 1D oraz 2D.
12. Gwarancja producenta min. 24 miesiące.

3.5. Dostawa urządzenia wielofunkcyjnego (1 szt.).

Minimalne parametry techniczne urządzenia wielofunkcyjnego:

1. Urządzenie musi zapewniać możliwość drukowania, skanowania i kopiowania.
2. Technologia druku: kolorowa, atramentowa.
3. Format druku i skanu: min. A4.
4. Druk i skan dwustronny.
5. Automatyczny podajnik dokumentów.
6. Min. dwa dodatkowe podajniki papieru, w tym min. jeden ładowany od przodu urządzenia dla min. 250 arkuszu papieru.
7. Możliwość ręcznego uzupełniania atramentu za pomocą butelek z atramentem dostępnych w technologii producenta urządzenia.

8. Możliwość bezpośredniego wydruku z USB przez port USB.
9. Rozdzielczość druku w kolorze i mono: min. 600x600 dpi.
10. Możliwość skanowania w kolorze.
11. Optyczna rozdzielczość skanowania: min. 600x600 dpi.
12. Skanowanie do e-mail oraz do plików w formacie BMP, JPEG, TIFF, PDF, PNG.
13. Dotykowy panel LCD sterujący urządzeniem.
14. Karta sieciowa LAN, karta bezprzewodowa WI-FI umożliwiająca zdalny wydruk z urządzeń.
15. Automatyczne kopiowanie dwustronne.
16. Wydajność tuszu czarnego – min. 7 000 stron A4 według danych producenta.
17. Wydajność tuszu kolorowego – min. 6 000 stron A4 według danych producenta.
18. Możliwość drukowania kopert.
19. Obsługa rozmiarów papieru: A4, A5, A6.
20. Obsługa papieru o gramaturze do 160 g/m².
21. Gwarancja producenta min. 24 miesiące.

3.6. Dostawa kluczy U2F (4 szt.).

Minimalne parametry techniczne urządzenia:

1. Komunikacja: USB type A, 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. Musi posiadać możliwość weryfikacji obecności użytkownika (tzw. “User Presence”) - np. przycisk lub element dotykowy
12. Wykorzystywanie jako tag NFC (np. uruchamianie innych urządzeń, kontrola dostępu).
13. Gwarancja: min. 12 miesięcy gwarancji producenta.

3.7. Dostawa serwera (2 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa RACK o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 2,5 cala wraz z kompletem szyn umożliwiających montaż w szafie RACK.
2. Płyta główna z możliwością zainstalowania jednego procesora.
3. Zainstalowany jeden procesor klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 90 punktów w teście SPECrate2017_fp_base dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej. Zamawiający żąda załączenia dokumentu potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności do dokumentacji powykonawczej.

4. Pamięć RAM: min. 32 GB w najnowszej technologii oferowanej przez producenta w dwóch kościach pamięci, co najmniej 20 wolnych slotów na pamięć.
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. trzy sloty PCIe min. Gen 3.
7. Interfejsy sieciowe: min. 4 porty RJ-45 1 GbE oraz min. 2 porty RJ-45 10 GbE.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane min. 2 dyski twarde Hot-Plug SAS o pojemności min. 300 GB każdy o min. prędkości zapisu 12 Gb/s oraz min. 2 dyski twarde Hot-Plug SSD SATA o pojemności min. 960 GB każdy o min. prędkości zapisu 6 Gb/s . W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0/1/10/5/50/6/60.
10. Wbudowane porty: min. 3 porty USB, z czego min. 2 w technologii 3.0, 1 port VGA.
11. Dodatkowe karty: zintegrowana karta graficzna.
12. Wentylatory: Redundantne typu Hot Plug.
13. Zasilacze: Redundantne typu Hot Plug.
14. 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) autentykacja dwuskładnikowa;
    4) wirtualną konsolę z dostępem do myszy, klawiatury,
    5) wsparcie dla IPv6,
    6) wsparcie dla SNMP; IPMI, SSH, SSL,
    7) integracja z Active Directory.
15. 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.
16. Dokumenty potwierdzające 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 140001 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 dokumentów potwierdzających spełnienie przez oferowaną jednostkę centralną i monitor oraz jego/ich producenta/producentów w zakresie określonym powyżej do dokumentacji powykonawczej.

17. Gwarancja: min. 36 miesięcy gwarancji producenta realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia.

3.8. Dostawa licencji serwerowego systemu operacyjnego (SSO) wraz z licencjami dostępowymi (2 szt.).

Wykonawca jest zobowiązany dostarczyć następujące oprogramowanie:

1. Oprogramowanie klasy Microsoft Windows Serwer Standard 2022 w liczbie szt. 2 (dwie osobne licencje, a nie tylko możliwość instalacji dwóch instancji w ramach jednej licencji) lub równoważne zgodnie z poniżej określonymi warunkami równoważności umożliwiające instalację na dwóch oferowanych serwerach fizycznych, z których każdy jest w konfiguracji jednoprocesorowej, a każdy procesor posiada oferowaną przez Wykonawcę liczbę rdzeni. Licencje muszą przeznaczona dla instytucji rządowych typu government.
2. Oprogramowanie klasy Microsoft Windows Server 2022 Device CAL lub równoważne dla 30 urządzeń umożliwiających jednoczesne korzystanie z zasobów dwóch serwerów.

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

1. Licencje muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w dwóch środowiskach fizycznych oraz maksymalnie czterech wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji (po 2 środowiska wirtualne na każdy fizyczny serwer).
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64 TB 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.
21. Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2021/2016.

3.9. Dostawa urządzenia NAS wraz z dyskami (1 szt.).

1. Obudowa do szafy RACK o rozmiarze nieprzekraczającym 2U.
2. Procesor wielordzeniowy.
3. Pamięć RAM: min. 2 GB.
4. Funkcje: wsparcie dla wirtualizacji, scentralizowana pamięć masowa na dane, backup, udostępnianie i przywracanie systemu po awarii.
5. Możliwość zainstalowania łącznie 4 dysków 3,5 calowych, min. SATA 3 - 6 Gb/s.
6. Zainstalowane dyski: min. 4 x 4 TB SATA 6 GB/s przeznaczonych dla systemów NAS pracujących w trybie ciągłym z czasem MTBF min. 1 000 000 godzin.
7. Poziom RAID: 0,1,5,6,10.
8. Obsługa systemów plików: Btrfs, ext4, NTFS i inne.
9. Kompatybilność dysków: 3,5-calowe dyski twarde SATA; 2,5-calowe dyski twarde SATA; 2,5-calowe dyski SSD SATA.
10. Obsługa dwóch połączeń RJ45 1Gb/s z obsługą Link Aggregation IEEE 802.3ad.
11. Porty USB: min. 2x USB 3.x.
12. Szyny do montażu w szafie RACK.
13. Gwarancja producenta: min. 36 miesięcy 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.

3.10. Dostawa urządzenia UTM (3 szt.).

Zamawiający przewiduje dostawę dwóch typów urządzeń – TYP A (1 szt.) oraz TYP B (2 szt.).
Urządzenia powinny dawać możliwość pracy w trybie site to site.

UWAGA! TERMIN DOSTAWY URZĄDZEŃ UTM WYNOSI 90 DNI OD DNIA ZAWARCIA UMOWY.

Minimalne parametry techniczne UTM TYP A (1 szt.):

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 oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS.

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. 20 Gbps.
2. Musi obsługiwać min. 1 500 000 jednoczesnych połączeń.
3. Musi obsługiwać co najmniej 500 jednoczesnych połączeń SSL VPN.
4. Przepustowość IPS: min. 2,6 Gbps.
5. Wydajność SSL VPN: min. 1 Gbps.
6. Automatyczna aktualizacja plików sygnatur antywirusowych.
7. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
8. Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.
9. Automatyczna aktualizacja sygnatur IPS.
10. IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.
11. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
12. Ilość interfejsów sieciowych: minimum 12 portów Gigabit Ethernet RJ-45 oraz min. 2 porty 10 Gigabit Ethernet SFP+. Interfejsy te powinny być skonfigurowane jako jeden z trzech rodzajów wymaganych stref bezpieczeństwa.
13. Administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania.
14. 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, IMAP, 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.
k. Analiza ruchu szyfrowanego protokołem SSH.

15. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
16. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
17. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
18. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
19. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
20. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
21. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
22. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
23. 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 w okresie gwarancji urządzenia.
24. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
25. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
26. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
27. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
28. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
29. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
30. Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
31. Urządzenie powinno mieć możliwość generowania raportów.
32. 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.
33. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
34. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

35. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
36. 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.
37. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
38. 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 gwarancji urządzenia.
39. Gwarancja producenta min. 60 miesięcy. Gwarancja powinna obejmować również możliwość wymiany urządzenia na nowe w przypadku wady urządzenia UTM.

Minimalne parametry techniczne UTM TYP B (2 szt.):

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 oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS.

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. 5 Gbps.
2. Musi obsługiwać min. 700 000 jednoczesnych połączeń.
3. Musi obsługiwać co najmniej 200 jednoczesnych połączeń SSL VPN.
4. Przepustowość IPS: min. 1 Gbps.
5. Wydajność SSL VPN: min. 450 Mbps.
6. Automatyczna aktualizacja plików sygnatur antywirusowych.

7. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
8. Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.
9. Automatyczna aktualizacja sygnatur IPS.
10. IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.
11. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
12. Ilość interfejsów sieciowych: minimum 3 porty Gigabit Ethernet RJ-45. Interfejsy te powinny być skonfigurowane jako jeden z trzech rodzajów wymaganych stref bezpieczeństwa.
13. Administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania.
14. 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, IMAP, 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.
    k. Analiza ruchu szyfrowanego protokołem SSH.
15. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
16. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
17. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
18. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
19. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
20. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
21. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
22. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
23. 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 w okresie gwarancji urządzenia.

24. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
25. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
26. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
27. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
28. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
29. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
30. Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
31. Urządzenie powinno mieć możliwość generowania raportów.
32. 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.
33. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
34. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
35. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
36. 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.
37. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
38. 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 gwarancji urządzenia.
39. Gwarancja producenta min. 60 miesięcy. Gwarancja powinna obejmować również możliwość wymiany urządzenia na nowe w przypadku wady urządzenia UTM.

3.11. Dostawa licencji oprogramowania do przechowywania i analizy logów (1 szt.).

Dla urządzenia UTM typu A Wykonawca jest zobowiązany dostarczyć licencję na oprogramowanie do przechowywania i analizy logów o parametrach minimalnych:

1. Oprogramowanie musi umożliwiać zbieranie i analizę zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach oferowanej infrastruktury UTMa typu A. Oferowane rozwiązanie musi być rozwiązaniem chmurowym.

2. Oprogramowanie musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzeń oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: listę najczęściej wykrywanych ataków; listę najbardziej aktywnych użytkowników, listę najczęściej wykorzystywanych aplikacji, listę najczęściej odwiedzanych stron www, listę krajów , do których nawiązywane są połączenia, listę najczęściej wykorzystywanych polityk Firewall, Informacje o realizowanych połączeniach IPSec.
3. Oprogramowanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
4. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
5. Oprogramowanie musi zapewniać cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
6. Oprogramowanie musi umożliwiać konfigurację powiadomień poprzez: e-mail oraz SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
7. Oprogramowanie musi umożliwiać generowanie raportów w formie plików pdf lub csv predefiniowanych lub według zadanych przez administratora parametrów.
8. Oprogramowanie musi umożliwiać generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres email.
9. Oprogramowanie musi umożliwiać zarządzanie lokalne z wykorzystaniem protokołów: HTTPS lub SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
10. Dostarczone oprogramowanie musi umożliwiać przechowywanie i analizę logów w okresie ostatnich 12 miesięcy.

3.12. Przeprowadzenie szkolenia online w zakresie SSO i urządzenia UTM (3 szt.).

Zamawiający przewiduje szkolenia w następujących obszarach merytorycznych:

1. W zakresie konfiguracji i administracji oferowanych urządzeń UTM.
2. W zakresie administracji, usług katalogowych i tożsamości oferowanego serwerowego systemu operacyjnego.

<u>Wymagania dla szkolenia w zakresie konfiguracji i administracji oferowanych urządzeń UTM.</u>
Uczestnik autoryzowanych szkoleń w zakresie konfiguracji i administracji urządzenia UTM uzyska kompetencje w zakresie poprawnej konfiguracji i zarządzania urządzeniem. Szkolenie powinno być przeprowadzone w systemie autoryzowanych szkoleń przez producenta dostarczonego urządzenia UTM. Szkolenie powinno zostać przeprowadzone przez osobę z tytułem Certified Trainer certyfikowaną przez producenta urządzenia UTM.

Ramowy zakres szkolenia:

1. Konfiguracja trybu pracy urządzenia router/NAT.

2. Zarządzanie aktualizacjami oraz backup.
3. Budowa i optymalizacja reguł zapory sieciowej.
4. Konfiguracja systemu wykrywania włamań (IDS/IPS).
5. Monitorowanie wykorzystania aplikacji i blokowanie malware/ransomware.
6. Konfiguracja modułu filtrowania stron www i profili antyspam.
7. Zarządzanie wyciekiem danych DLP.
8. Konfiguracja wielu łączy internetowych WAN.
9. Raportowanie i analiza zdarzeń.
10. Konfiguracja połączeń tunelowych Site-to-Site IPsec VPN.
11. Zarządzanie dostępem zdalnym SSL-VPN w oparciu o dwu stopniowe metody uwierzytelniania.
12. Zarządzanie mechanizmami routingu.
13. Konfiguracja systemy ochrony przed atakami DDoS.
14. Zaawansowana analiza logów i zdarzeń.
15. Diagnostyka i rozwiązywanie problemów.

Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolona 1 osoba - pracownik Urzędu Gminy Gorzkowice.
2. Szkolenie musi być prowadzone przez instytucję uprawnioną do realizacji szkoleń autoryzowanych.
3. Szkolenie musi odbywać się w formie szkolenia w trybie on-line.
4. Szkolenie musi być prowadzone w języku polskim, Zamawiający dopuszcza materiały w języku angielskim.
5. Szkolenie powinno trwać minimum 16 godzin szkoleniowych.

<u>Wymagania dla szkolenia w zakresie administracji, usług katalogowych i tożsamości oferowanego serwerowego systemu operacyjnego.</u>

Uczestnik autoryzowanych szkoleń w zakresie administracji, usług katalogowych i tożsamości oferowanego serwerowego systemu operacyjnego uzyska kompetencje w zakresie administracji, poprawnej konfiguracji usług katalogowych oraz zarządzania tożsamością. Szkolenie powinno być przeprowadzone w systemie autoryzowanych szkoleń przez producenta dostarczonego serwerowego systemu operacyjnego. Szkolenie powinno zostać przeprowadzone przez osobę z tytułem Certified Trainer certyfikowaną przez producenta serwerowego systemu operacyjnego.

Ramowy zakres szkolenia:

1. Wprowadzenie do administracji serwerowego systemu operacyjnego.
2. Usługi tożsamości serwerowego systemu operacyjnego.
3. Usługi infrastruktury sieci serwerowego systemu operacyjnego.
4. Serwery plików i zarządzanie pamięcią.
5. Wirtualizacja i kontenery.
6. System wysokiej niezawodności.
7. Odtwarzanie awaryjne.
8. Ochrona serwerowego systemu operacyjnego
9. RDS serwerowego systemu operacyjnego.
10. Zdalny dostęp i usługi sieciowe.

11. Monitorowanie serwera i sprawności.
12. Ulepszanie i migracja.
13. Instalowanie i konfigurowanie kontrolerów domeny.
14. Zarządzanie obiektami w usługach AD DS.
15. Zarządzanie zaawansowaną infrastrukturą AD DS.
16. Implementowanie lokacji usług AD DS oraz konfigurowanie replikacji i zarządzanie nią.
17. Wdrażanie zasad grupy.
18. Zarządzanie ustawieniami użytkownika za pomocą zasad grupy.
19. Zabezpieczanie usług domenowych Active Directory.
20. Wdrażanie usług AD CS i zarządzanie nimi.
21. Wdrażanie certyfikatów i zarządzanie nimi.
22. Wdrażanie i administrowanie usługami AD FS.
23. Wdrażanie i administrowanie usługi AD RMS.
24. Monitorowanie usług AD DS, zarządzanie nimi oraz odzyskiwanie danych.

Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolona 1 osoba - pracownik Urzędu Gminy Gorzkowice.
2. Szkolenie musi być prowadzone przez instytucję uprawnioną do realizacji szkoleń autoryzowanych.
3. Szkolenie musi odbywać się w formie szkolenia w trybie on-line.
4. Szkolenie musi być prowadzone w języku polskim, Zamawiający dopuszcza materiały w języku angielskim.
5. Szkolenie powinno trwać minimum 80 godzin szkoleniowych.