GKŚO.I.271.9.2022

Załącznik nr 5 do SWZ Opis przedmiotu zamówienia.

OPZ zawiera opis przedmiotu zamówienia dla Części I, II i III.

1. **Część I: Dostawa specjalistycznego oprogramowania do zarządzania urządzeniami końcowymi (Punkt 1) i oprogramowania serwera wraz z częściami (Punkt 2)**

**Punkt 1 - Dostawa specjalistycznego oprogramowania do zarządzania urządzeniami końcowymi**

Przedmiotem jest dostawa oprogramowania wraz z licencjami dla 25 stanowisk komputerowych (25 sztuk) oraz wykonanie wdrożenia zakupionego oprogramowania celem podniesienia poziomu cyberbezpieczeństwa systemu informatycznego posiadanego przez Zamawiającego.

**1. Definicje**

Zamawiający dokonał opisu przedmiotu z wykorzystaniem następujących definicji:

|  |  |  |
| --- | --- | --- |
| **Lp** | **Termin**  | **Definicje**  |
| 1 | **Aktualizacje**  | Jakiekolwiek uaktualnienia Oprogramowania, dostarczone w związku z zapewnieniem Wsparcia Technicznego, w tym wydania uzupełniające, patche, zmiany, poprawki oraz inne dostosowania w tym wskazane w OPZ, zapewniające prawidłowe korzystanie z takiego oprogramowania. |
| 2 | **Dokumentacja techniczna** | Wszelka dokumentacja dostarczona lub wykonana na podstawie Umowy w szczególności dokumentacja niezbędna do korzystania z Oprogramowania w tym techniczna oraz użytkowa. |
| 3 | **Dni robocze** | dni ustawowo wolne od pracy na terenie Rzeczypospolitej Polskiej. |
| 5 | **Oprogramowanie** | Oprogramowanie opisane w pkt 2 OPZ. |
| 6 | **OPZ** | Niniejszy Opis Przedmiotu Zamówienia. |
| 7 | **Producent**  | Producent Oprogramowania, oferowanego przez Wykonawcę. |
| 8 | **Umowa** | Umowa w sprawie zamówienia publicznego zawarta między Zamawiającym a Wykonawcą. |

**2. Przedmiot zamówienia**

1. Przedmiotem zamówienia jest dostawa licencji na Oprogramowanie służąca poprawie bezpieczeństwa systemów informatycznych Zamawiającego spełniającego wymagania opisane w niniejszym OPZ, wraz z zapewnieniem Wsparcia Technicznego dla dostarczonego Oprogramowania.
2. O ile nie zaznaczono inaczej, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
3. Zamawiający może wykonywać uprawnienia z rękojmi niezależnie od uprawnień wynikających z gwarancji jakości.
4. Wykonawca powinien posiadać status Partnera Producenta Oprogramowania z zastrzeżeniem, że jeśli Producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga aby Wykonawca posiadał poziom partnerstwa nie niższy niż drugi licząc od najwyższego poziomu partnerstwa w hierarchii poziomów stosowanych przez Producenta.
5. Wymóg dotyczy Wykonawcy i jego ewentualnego podwykonawcy. Wykluczona jest sytuacja aby tylko jeden z tych podmiotów posiadał wyżej wskazany poziom partnerstwa.
6. Oprogramowanie dostarczone przez Wykonawcę nie może naruszać bezpieczeństwa publicznego lub istotnego bezpieczeństwa publicznego państwa, mając na względzie fakt, iż Zamawiający art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa należy do Krajowego systemu cyberbezpieczeństwa, którego celem zgodnie z art. 3 wyżej wskazanej ustawy jest zapewnienie odpowiedniego poziomu cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenie usług kluczowych i usług cyfrowych przez osiągnięcie odpowiedniego poziomu do świadczenia tych usług i obsługi incydentów. Tym samym dostarczone oprogramowanie musi być zgodne z wymogami krajowego systemu cyberbezpieczeństwa.

**3. Dostawa.**

1. Dostawa ma zostać dokonana w dni robocze w godzinach od 7.30 do 15.00.
2. Dostarczone licencje na Oprogramowanie musza obejmować dostęp do najnowszej wersji tego oprogramowania udostępnionej przez Producenta.
3. Licencje wraz z dostarczonym Oprogramowaniem musza pochodzić z oficjalnego kanału dystrybucji ich Producenta.
4. Wykonawca jest zobowiązany do przekazania Zamawiającemu aktualnego zestawienia w formacie xls wszystkich dostarczonych pozycji w zakresie Oprogramowania zawierających: oznaczenie producenta (part numer), pełna nazwa produktu, metryka licencyjna, wersja i edycja oprogramowania, rodzaj licencji, okres obowiązywania licencji, okres wsparcia technicznego, poziom wsparcia technicznego, cena jednostkowa netto, stawka podatku VAT, cena jednostkowa brutto.
5. Minimalne wymogi dla wsparcia technicznego.

Wykonawca zobowiązuje się dokonać dostawy Oprogramowania wraz z zapewnieniem dla Zamawiającego Wsparcia Technicznego dla dostarczonego Oprogramowania i wszelkich licencji udzielanych w celu wykonania umowy – przez okres 36 miesięcy od dnia odbioru Oprogramowania.

1. Minimalny zakres Wsparcia Technicznego obejmuje:
* dostęp za pośrednictwem serwisu www do aktualnej dokumentacji technicznej i bazy wiedzy publikowanej i udostępnianej przez Producenta;
* dostęp za pośrednictwem www do obrazów (plików) do pobrania zawierających poprawki/aktualizacje/wersje instalacyjne Oprogramowania niezwłocznie po ich udostepnieniu przez producenta oprogramowania.

**4. Terminy realizacji**

Wykonawca zobowiązany będzie zrealizować dostawę licencji na Oprogramowanie w terminie 5 dni roboczych od dnia zawarcia Umowy.

**5. Szczegółowe wymogi dla Oprogramowania.**

**Informacje Ogólne.**

* Dostarczone licencje na oprogramowanie są bezterminowe.
* Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
* Oprogramowanie współpracuje z serwerem SQL Server 2019, SQL Server 2017, SQL Server 2016 SP3, SQL Server 2014 SP3, Oracle 19c, Oracle 12c R2.
* Oprogramowanie serwera aplikacji umożliwia wysyłanie powiadomień mailowych.
* Oprogramowanie posiada system ról, dzięki któremu jest możliwe przypisywanie wybranych grup stanowisk do poszczególnych użytkowników konsoli.
* Wszelkie raporty, zestawienia oraz funkcje grupowe obejmują wtedy tylko w/w przypisane grupy stanowisk.
* Oprogramowanie realizuj zarządzanie wszystkimi modułami systemu z poziomu tej samej konsoli zarządzającej.
* Oprogramowanie agenta realizuje wszystkie wymagane funkcjonalności z poziomu jednej instancji usługi lub procesu bez wykorzystywania aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
* Oprogramowanie pozwala export do Excel'a dowolnego widoku konsoli administracyjnej.
* Oprogramowanie pozwala zarządzać z jednej konsoli zarówno stacjami klienckimi, serwerami jak i urządzeniami mobilnymi z systemami operacyjnymi Android oraz iOS.
* Oprogramowanie, niezależnie od ilości funkcjonalności lub zarządzanych urządzeń końcowych działa w oparciu o 1 oprogramowanie typu Agent na urządzeniu końcowym.
* Oprogramowanie posiada architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta.
* Oprogramowanie działa na minimalnych wymaganiach sprzętowych:

Wymagania sprzętowe:

- procesor minimum 2 rdzenie;

- 8 GB wolnej pamięci- rekomendowane 16 GB;

- karta sieciowa min 1 Gigabit;

- przestrzeń w celu instalacji: minimum 5 GB;

Wymagane oprogramowanie dla Serwera:

- Serwer OS - od Windows Server 2016 (64-Bit);

- od 5 GB wolnej przestrzeni dyskowej na instalacje serwera;

- Baza Danych - od SQL Server 2014 SP3;

Wymagania dla stacji klienckiej:

- od Intel Pentium IV procesor z 1GHz;

- od 256 MB wolnej pamieci RAM;

- od 200 MB wolnego miejsca na dysku twardym;

* Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
* Oprogramowanie umożliwia dystrybucję dowolnego oprogramowania, nie tylko paczek MSI, ale również takich jak InnoSetup, InstallShield i inne.
* Oprogramowanie umożliwia automatyzowanie instalatorów wraz z możliwością customizowania instalatorów w taki sposób, żeby można było nadpisywać pola opisowe, zmieniać dowolne wartości, w tym miejsce zapisu na dysku na urządzeniu końcowym.
* Oprogramowanie umożliwia administratorowi zautomatyzowanie procesu instalacji, w taki sposób, by nagrany został cały proces instalacji w taki sposób, by w momencie instalacji na urządzeniu końcowym nie było wymagane podanie jakichkolwiek opcji.
* Oprogramowanie musi umożliwiać zautomatyzowania zdalnej instalacji dowolnego oprogramowania w taki sposób, by oprogramowanie można było zainstalować zdalnie w trybie cichym (Silent Mode) lub graficznym.
* Oprogramowanie musi umożliwiać dodawanie takich opcji w instalatorach jak:

- blokowanie klawiatury i myszki,

- zmiany w ustawieniach w rejestracji na stacjach klienckich,

- działania na plikach I folderach na stacji klienckiej,

- dodanie skryptu np. w PowerShellu

- zatrzymanie/wznowienie usług oraz procesów na stacji klienckiej"

* Zdalna dystrybucja oprogramowania musi wykorzystywać natywną inteligencję instalatora. Nie może wykorzystywać Snapshotingu.
* Zdalna dystrybucja oprogramowania musi mieć opcje schedullingu:

- w zadanym przedziale czasowym;

- wprowadzenie cykliczności (np. wybrany dzień tygodnia o wybranej godzinie);

- połączenie dwóch powyższych;

- na żądanie w danym momencie;

* Oprogramowanie musi umożliwiać wzbudzanie stacji klienckich metodą Wake-On-LAN.
* Oprogramowanie musi umożliwiać administratorowi podgląd co do Statusu danego taska per maszyna w czasie rzeczywistym, a w przypadku błędu w wykonaniu - zwrócić informację co było przyczyną błędu.
* W przypadku dokupienia nowych funkcjonalności/modułów oprogramowania, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
* W przypadku zwiększenia ilości zarządzanych maszyn w dowolnym momencie, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
* Oprogramowanie musi umożliwiać zdalną dystrybucję oprogramowania z jednej konsoli zarówno na stacjach klienckich (jak PC I laptop/notebook) jak i urządzeniach mobilnych z systemem Android.
* Oprogramowanie dostarczy administratorowi informacji o dacie ostatniego uruchomienia aplikacji na stacji klienckiej PC per każda stacja kliencka.
* Dystrybucja agentów na stacjach klienckich musi być możliwa zarówno w sposób automatyczny jak i ręczny.
* Oprogramowanie umożliwia integrację z Active Directory oraz pobranie informacji z AD I automatyczne zarejestrowanie urządzeń z AD w serwerze.
* Zarówno w przypadku stacji klienckich PC jak I urządzeń mobilnych z systemem Android, oprogramowanie musi umożliwiać administratorowi dostarczenie użytkownikowi końcowemu interfejsu typu self-service, w którym będzie miał listę dostępnych instalatorów z możliwością ich dociągnięcia i zainstalowania; Musi istnieć możliwość automatycznej personalizacji takiej listy per grupa lub konkretne urządzenie końcowe.
* Oprogramowanie musi posiadać otwarte API do integracji z zewnętrznymi serwerami, np. poprzez Web Service'y.
* Oprogramowanie musi umożliwiać również tworzenie własnych skryptów, które następnie można automatycznie instalować na urządzeniach końcowych, typu stacja kliencka.
* W przypadku automatycznej zdalnej instalacji oprogramowania na stacjach klienckich, oprogramowanie musi dać opcje tworzenia listy oprogramowania zależnego, tzn. w przypadku gdy do poprawnego działania aplikacja X wymaga instalacji aplikacji Y, Oprogramowanie musi dawać opcję ustalenia listy takiego oprogramowania zależnego na poziomie konfiguracji aplikacji X z poziomu konsoli. W przypadku dystrybucji aplikacji X, gdy na stacji klienckiej nie będzie zainstalowana aplikacja Y, serwer automatycznie wypchnie na tą stację paczkę instalacyjną aplikacji Y .
* Oprogramowanie musi dawać administratorowi możliwość przypisywania wykonywania tasków zarówno na urządzeniach końcowych spełniających wybrane warunki dynamiczne (np. Wolne miejsce na dysku C, wersja systemu operacyjnego itp.), jak i urządzeniach przypisanych do konkretnych grup, jak w AD.
* Oprogramowanie musi posiadać środowisko skryptowe, umożliwiające tworzenie własnych skryptów i w łatwej dystrybucji skryptów z poziomu konsoli.
* Oprogramowanie musi posiadać możliwość automatycznego skanowania komputerów i serwerów pod kątem podatności i przestrzegania wytycznych dotyczących bezpieczeństwa i zgodności z wykorzystaniem standardowych zbiorów reguł, które są utrzymywane przez certyfikowane organizacje i firmy zajmujące się bezpieczeństwem cybernetycznym (proces wyszukiwania podatności musi bazować na minimum 25000 stale aktualizowanych reguł) oraz reguł definiowanych przez użytkownika.
* Oprogramowanie musi pozwalać na przegląd sprzętu, oprogramowania i dowolnych danych przedsiębiorstwa. Zawierać się w tym powinny następujące możliwości oprogramowania: szybka inwentaryzacja sprzętu, kompleksowa inwentaryzacja oprogramowania, transparentne przedstawienie wyników inwentaryzacji, rozpoznawanie niedozwolonego oprogramowania, tworzenie raportów zawierających niezbędne dane. Możliwość dostosowanie jakie dane są rejestrowane przez oprogramowanie z uwzględnieniem RODO.
* Oprogramowanie musi pozwalać na identyfikację urządzeń SNMP, takich jak drukarki, routery, przełączniki i inne urządzenia sieciowe, a także na wizualizację topologii sieci. W tym zawiera się: automatyczne skanowanie sieci firmowej, rejestracja wszystkich urządzeń sieciowych kompatybilnych z protokołem SNMP za pomocą skanera SNMP, możliwość tworzenia reguł definiowanych przez użytkownika w edytorze graficznym, dostępny standardowy zbiór reguł do definiowania urządzeń, możliwość indywidualnego dopasowania i rozszerzenia zbioru reguł w dowolnym momencie, przejrzystość dzięki wizualnemu przedstawieniu topologii sieci w postaci mapy systemu IT.
* Oprogramowanie musi posiadać funkcję zautomatyzowanego zarządzania mobilnymi urządzeniami końcowymi, automatycznego zarządzanie zgodnie ze standardowymi procedurami i pozwalać na definiowanie i egzekwowanie reguł bezpieczeństwa. Oprogramowanie musi posiadać odpowiednie aplikacje na systemy Android i iOS pozwalające na komunikację z i zarządzanie urządzeniami mobilnymi, które muszą być dostępne do zainstalowania z poziomu oficjalnego sklepu z aplikacjami dla danego systemu operacyjnego.
* Oprogramowanie musi pozwalać na bezpieczne rozdzielenie danych prywatnych i biznesowych na urządzeniach mobilnych, zapewniać bezpieczeństwo danych podczas użytkowania urządzenia dla celów prywatnych, zapewnić obsługę Aapple iOS User Enrollment oraz Android Enterprise Workprofile. Musi także umożliwiać wykorzystanie opcji oferowanej przez Android Enterprise w celu utworzenia osobnych profili użytkownika, bez konieczności korzystania z rozwiązań kontenerowych zarządzanych przez stronę trzecią.
* Oprogramowanie musi pozwalać na udostępnianie aktualizacji i patch’y wielu aplikacji w postaci gotowych do dystrybucji, przetestowanych pakietów oprogramowania. W tym musi zawierać się: gotowe do dystrybucji pakiety oprogramowania do aktualizacji i instalacji patch’y, szybka dostępność aktualizacji istotnych dla bezpieczeństwa, stała aktualność i bezpieczeństwo aplikacji.
* Oprogramowanie musi pozwalać na wizualizację i zarządzanie natywnymi funkcjami bezpieczeństwa systemu operacyjnego. W tym zawiera się: transparentne zarządzanie szyfrowaniem BitLocker, szczegółowy przegląd funkcji zabezpieczeń programu Defender dla wszystkich punktów końcowych, automatyczne aktualizacje plików ze wzorcami wirusów, oraz centralne zarządzanie metody usuwania złośliwego oprogramowania.
* Oprogramowanie musi pozwalać na bezpośrednie połączenie z pulpitem komputerów w sieci umożliwiające zdalne wyświetlanie zawartości ekranu użytkownika, który w tym czasie może kontynuować pracę jak również zdalne sterowanie klawiaturą i myszą w systemie docelowym. Wyżej opisana funkcjonalność musi działać zarówno w przypadku komputerów jak i systemów serwerowych. Zdalny dostęp musi być realizowany zgodnie z przepisami RODO – tzn. jest on możliwy tylko wówczas, gdy nikt nie jest zalogowany w systemie lub po udzieleniu zgody wprost przez użytkownika.

**Architektura Platformy.**

* Oprogramowanie wspiera MsSQL-Server (również w wersji Express);
* Oprogramowanie posiada konsolę zarządzającą jako część oprogramowania (nie tylko interfejs webowy);
* Oprogramowanie posiada Agenta dla systemów klienckich Windows od Windows oraz Windows Server;
* Oprogramowanie wspiera więcej niż jeden serwer-repozytorium (DIP-Server) ;
* Oprogramowanie wspiera PXE-Relay;
* Oprogramowanie wspiera WakeUp-Points;
* Oprogramowanie posiada możliwość integracji z Active Directory;

**Komunikacja ( server-clients).**

* Oprogramowanie obsługuje niewielką przepustowością łącza dla kontroli agentów i przesyłania informacji o statusach
* Oprogramowanie umożliwia indywidualną synchronizację pomiędzy pojedynczymi serwerami repozytorium (ograniczenie czasowe i przepustowości łącza)
* Oprogramowanie posiada dostęp read-only do AD, bez rozszerzeń schematu
* Oprogramowanie umożliwia wybudzanie stacji klienckich Wake-On-LAN
* Oprogramowanie wspiera zadania/Joby Push i Pull (łącznie z Shutdown)
* Oprogramowanie umożliwia komunikację bez konieczności zestawiania połączenia VPN z urządzeniami, które są poza siecią poprzez bramkę Proxy instalowaną w DMZ. Bramka Proxy musi stanowić integralną część Oprogramowania. Komunikacja pomiędzy bramką a agentem, jak i bramką a serwerem musi odbywać się poprzez HTTPS

**Operacje wykonywane przez Oprogramowanie.**

* Oprogramowanie umożliwia pracę wielu administratorów równocześnie na jednej konsoli;
* Oprogramowanie posiada wsparcie dla LAN, zdalne i OFFLINE stanowiska pracy;
* Oprogramowania umożliwia wyświetlenie informacji i stanu/statusów dostępnych w czasie rzeczywistym ze znacznikiem czasowym;
* W przypadku zakończenia wykonania zadania na stacji z błędem, administrator widzi w konsoli administracyjnej szczegółowe przyczyny błędu, które spowodowały niewykonanie danego zadania;
* Komunikaty o błędach są generowane natychmiast (wraz z informacją o docelowym systemie OS);
* Dowolnie definiowane dodatkowe pola (Variable/Zmienne) przechowywane w tej samej bazie danych (np. Informacje o gnieździe sieciowym, danych dotyczących wynajmu, informacje supportowe)
* Rozbudowane funkcjonalności dotyczące zarządzania uprawnieniami;
* Wsparcie dla grup dynamicznych na potrzeby indywidualnych informacji/widoku;
* Oprogramowanie musi zawierać opcję ukrywania danych osobowych użytkowników (takich jak imię, nazwisko, login) dla wybranych administratorów;
* Oprogramowanie musi umożliwiać przyznawanie i blokowanie dostępu do wybranej części infrastruktury oraz wybranych części funkcjonalności oprogramowania wskazanym administratorom.

**Minimum możliwości w zakresie zadań jakie powinno spełniać oprogramowanie.**

* Oprogramowanie umożliwia wysyłanie polecenia w trybie "Push";
* Oprogramowanie umożliwia wysyłanie polecenia w trybie "Pull";
* Oprogramowanie umożliwia wysyłanie polecenia w trybie "shutdown".;
* Oprogramowanie pozwala na indywidualną interakcję użytkownika w trakcie wykonywania zadania uruchomionego przez administratora w trybach: opóźnienie, odmowa, przypomnienie o instalacji;
* Oprogramowanie umożliwia wysyłanie polecenia Wake-on LAN;
* Oprogramowanie umożliwia automatyczne generowanie i wysyłanie powtarzających się zadań (recurring Jobs);
* Oprogramowanie umożliwia uruchomienie zadania z poziomu użytkownika końcowego poprzez Kiosk samoobsługowy SelfService (dostępny przez Web);
* Zadania mogą być inicjowane z poziomu aplikacji selfservice - konsoli Webowej;
* Zawartość aplikacji SelfService (Kiosku) może być definiowana zarówno per User/Grupa Userów jak i per PC/Organisation Unit;

**Instalacja Oprogramowania (uwagi i wymagania minimalne).**

* Kreator do tworzenia pakietów, w skład których wchodzi różnorodne oprogramowanie;
* Detekcja oraz wsparcie kreatory dla wielu mechanizmów instalacji: MSI, InnoSetup, NullSoft, Wise-Installer i inne;
* Uzupełnienie instalacji oprogramowania na urządzeniu końcowym o dodatkowe kroki ze strony użytkownika końcowego (np.: deaktywacja okna powitalnego, itp);
* Integracja procedury odinstalowania;
* Natywna instalacja pakietów (a nie tylko wrap aplikacji w innym skrypcie instalacyjnym);
* Transparentna instalacja (w Logach znajduje się informacja dotycząca instalacji np.: msiexec.exe /i \\...\software-xyz.msi /qn /noreboot);
* Indywidualna konfiguracja zależności (np.:uprzednia instalacja .net (w przypadku, jeśli takowa nie miała jeszcze miejsca), następnie instalacja docelowego oprogramowania);
* Ustawianie zachowań w trakcie Reboot również dla oprogramowania;
* Możliwość użycia własnych skryptów, żeby np: customizować Linki, Rejestry, Working Directories, itd.;
* Użycie narzędzia do tworzenia własnych skryptów w celu tworzenia własnych pakietów instalacyjnych (np.: "kopiuj pliki z .. , stwórz ikonę Start");
* Dostarczenie narzędzia do nagrywania kroków instalacji oprogramowania, tak, by administrator mógł przejść wszystkie kroki instalatora i wypchnąć tak wyklikany instalator zdalne;
* Różnorodna weryfikacja instalacji (np.: jaka jest wartość zwrotna programu instalacyjnego, czy istnieje jakiś określony wpis do rejestru lub usługa);
* Ustawienie dowolnego kontekstu security/uprawnień z jakimi dana paczka ma zostać zainstalowana na urządzeniu końcowym;

**Automatyczna dystrybucja poprawek dla systemów MS / Patch Management**

* Oprogramowanie umożliwia dystrybucji patchy Windows bez WSUS;
* Oprogramowanie umożliwia triggerowanie z poziomu WSUS;
* Oprogramowanie umożliwia obsługę systemów operacyjne Microsoft — Windows Server 2008, Windows 7, Windows 8, Windows 10, Windows 11, Windows Server 2008R2, Windows Server 2012, Windows Server 2019 z natywną instalacją;
* Producent oprogramowania zapewnia stały dostęp do bazy danych z poprawkami Microsoft - baza jest dostępna dla Klienta z poziomu konsoli oprogramowania w dniu jej opublikowania przez Microsoft;
* Oprogramowanie umożliwia określenie ścisłych wymagań czasowych dla instalacji poprawek Microsoft i te wymagania kontrolować. Oprogramowanie nie wymaga ingerencji w reguły eksploatacji serwerów, a mimo to zapewnia ich odpowiednio szybkie zamknięcie w razie luk w zabezpieczeniach;
* Oprogramowanie pozwala administratorowi zarządzać aktualizacją systemów: możliwość sprawdzania tylko pod kątem brakujących poprawek i czy poprawki mają być od razu instalowane. Poprawki mogą być zatwierdzane automatycznie lub ręcznie. Oprogramowanie pozwala także ustalać reguły dla różnych grup w systemie IT;
* Oprogramowania pozwala by metodą drag and drop w środowisku zgodnym z MMC określać, w jakich systemach mają być instalowane poprawki. W taki sam sposób definiowane są również automatyczne instalacje i sytuacje, w których administrator ma być wcześniej pytany o zgodę. Oprogramowanie automatycznie pobiera wszystkie poprawki Microsoft i na żądanie automatycznie je rozprowadza w infrastrukturze Klienta zgodnie z wytycznymi administratora kreator skryptów, konfiguracji pakietów i autmatyzacja dowolnych procesów / Automate i Package Studio;
* Oprogramowanie pozwala na tworzenie plików transformacji (MST), które umożliwiają niezawodne dopasowanie do każdego MSI;
* Oprogramowanie pozwala na tworzenie kreatora instalacji dla dowolnej aplikacji - nie wymaga paczki MSI;
* Oprogramowanie pozwala tworzyć pakiety instalacyjne, gdzie w ramach procesu można zainstalować "n" aplikacji lub wykonać szereg dodatkowych funkcji związanych np. z inwentaryzacją;
* Oprogramowanie obsługuje wszystkie powszechnie dostępne na rynku systemy operacyjne Microsoft — Windows Vista i Server 2008, Windows 7, Windows 8, Windows10, Windows 11, Windows Server 2008R2, Windows Server 2012 i Windows 2019;
* Oprogramowanie umożliwia tworzenie plików sterujących (tansform);
* Oprogramowanie pozwala na automatyzacje niemal każdego procesu wykonywanego ręcznie na komputerze;
* Oprogramowania pozwala na proste tworzenie skryptów metodą drag and drop;
* Oprogramowanie zawiera standardowy zestaw poleceń;
* Oprogramowanie posiada możliwość sterowania również interfejsami niezgodnymi ze standardem (np. Java);
* Oprogramowanie posiada pomoc kontekstową;
* Oprogramowanie posiada tryb testowy step by step;
* Oprogramowanie zawiera gotowe repozytorium patch'y aplikacji firm trzecich, takie jak: Adobe, Java, przeglądarki, Team Viewer, Skype, Zoom etc. Repozytorium zawiera paczki bez AdWordsów ;
* Oprogramowanie umożliwia automatyczną aktualizację aplikacji firm trzecich;

**Punkt 2 - Dostawa oprogramowania i części komputerowych**

Szczegółowy Opis Przedmiotu Zamówienia Postępowanie „Dostawa sprzętu IT dla grantu Cyfrowa Gmina” realizowanego przez Gminę Kiwity.

1. Windows Exchange Server Standard 2019 (2szt.)
2. Windows Server CAL 2022 - Windows Server 2022 - 1 Device CAL (3szt.)
3. Windows Server CAL 2022 - Windows Server 2022 - 1 User CAL (25szt.)
4. Pamięć RAM 32GB (1szt.)
5. Wdrożenie/kopie zapasowe/konfiguracja klastra

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **1.** | **Pamięć operacyjna** | 1 x 32GB DIMM DDR4, 2666MHz  |
| **2.** | **System****operacyjny** | Oprogramowanie Windows Server 2022 lub równoważne Opis równoważności dla licencji Windows Server 2022:  1. Współpraca z procesorami o architekturze x64.  2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.  3. Możliwość budowania klastrów składających się z 64 węzłów.  4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory oraz 16 rdzeni.  5. Praca w roli klienta domeny Microsoft Active Directory.  6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2012.  7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.  8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).  9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory 11. Możliwość uruchomienia roli serwera stron WWW.  12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.  13. W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych.  14. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.  15. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).  16. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  17. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  18. Wbudowane wsparcie instalacji i pracy na wolumenach, które:  1) pozwalają na zmianę rozmiaru w czasie pracy systemu,  2) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  3) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  4) umożliwiają zdefiniowanie list kontroli dostępu (ACL).  19. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość  20. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  21. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET  22. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  23. Możliwość wykorzystania standardu http/2.  24. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  25. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  1) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  2) dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.  26. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.  27. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 28. Mechanizmy logowania w oparciu o:  1) login i hasło,  2) karty z certyfikatami (smartcard), 3) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 29. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:  1) określonych grup użytkowników,  2) zastosowanej klasyfikacji danych,  3) centralnych polityk dostępu w sieci,  4) centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.  30. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  31. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  32. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  33. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  34. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  35. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  1) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.  2) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  a. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  b. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  c. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  d. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.  3) Zdalna dystrybucja oprogramowania na stacje robocze.  4) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.  5) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  a. Dystrybucję certyfikatów poprzez http,  b. Konsolidację CA dla wielu lasów domeny,  c. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  d. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509 6) Szyfrowanie plików i folderów.  7) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec)  8) Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi  9) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  10) Serwis udostępniania stron WWW  11) Wsparcie dla protokołu IP w wersji 6 (IPv6).  12) Wsparcie dla algorytmów Suite B (RFC 4869).  13) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.  14) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.  15) Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  16) Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. 17) Mechanizmy wirtualizacji mające wsparcie dla:  a. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  b. obsługi ramek typu jumbo frames dla maszyn wirtualnych.  c. obsługi 4-KB sektorów dysków,  d. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  e. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  f. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  g. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.  18) Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.  19) Wsparcie dla rozwiązania Kubernetes. 20) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  21) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  22) Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB. 23) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  24) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  25) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF  26) Mechanizm konfiguracji połączenia VPN do platformy Azure.  27) Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.  28) Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.  29) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.  30) Możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Enterprise). 36. W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 7 godzin Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ.  37. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.  |
| **3.** | **Wdrożenie** | Wykonawca zobowiązuje się do wdrożenia oferowanego oprogramowania na dostarczony sprzęt, przeprowadzenia konfiguracji i integracji z istniejącą u zamawiającego infrastrukturą.Opis usługi:* usługa katalogowa, stanowiąca podstawę wielu usług.
* zawiera informacje o serwerach, użytkownikach, grupach i wszelkich innych obiektach w środowisku informatycznym.
* przechowuje dane o kontach użytkowników i komputerów, ich hasłach, a także informacje o lokalizacji usług (jak np. autodiscover dla MS Exchange, Office365 czy Skype for Business).
* jest narzędziem wykorzystywanym między innymi do realizacji centralnego zarządzania tożsamością i uwierzytelnianiem (logowanie) oraz definiowania reguł dostępu do zasobów (serwery plikowe/bazodanowe) w sieciach korporacyjnych, opartych o systemy Windows oraz Linux.

Centralne zarządzanie:* analiza potrzeb i doradztwo
* pomoc przy doborze urządzeń
* instalacja urządzeń w serwerowni (serwerowniach)

Bezpieczeństwo:* początkowa konfiguracja urządzenia obejmująca m. in. podstawową konfigurację sieci, konfigurację tabeli filtrowania, konfigurację VPN..
* konfigurację serwera DHCP i DNS;
* konfiguracja routera WAN i LAN;
* rekonfiguracja urządzenia;
* konfiguracja systemu wykrywania intruzów (IDS);
* konfiguracja systemu blokowania intruzów (IPS);

Uprawnienia:* aktualizacja oprogramowania sprzętowego;
* analiza logów;
* audyt bezpieczeństwa sieci;

Konfiguracja:* Utworzenie domeny.
* Utworzenie schematu organizacyjnego.
* Utworzenie folderów udostępnionych.
* Nadanie uprawnień do folderów po wcześniejszym uzgodnieniu macierzy uprawnień.
* Konfiguracja polityki zabezpieczeń.
* Konfiguracja kopii bezpieczeństwa.
* Instalacja drukarek oraz ploterów na serwerze oraz konfiguracja serwera wydruku.
* Podłączenie komputerów do utworzonej domeny – proces wykonywany etapowo.
* Migracja danych.
* Instalacja odpowiednich drukarek na komputerach.
* Konfiguracja VPN.
* Dokumentowanie wykonanych prac.
 |
| **4.** | **Kopie zapasowe** | Wykonawca przeprowadzi także konfigurację umożliwiającą tworzenie kopii zapasowych i przechowywanie ich na miejscu u zamawiającego. |
| **5.** | **Klaster****serwerów** | Niezależne od zainstalowanego na jednostce przetwarzania systemu operacyjnego, posiadające dedykowany port RJ-45 Gigabit Ethernet umożliwiające: * zdalny dostęp do graficznego interfejsu Web karty zarządzającej - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera)
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika - możliwość podmontowania zdalnych wirtualnych napędów
* wirtualną konsolę z dostępem do myszy, klawiatury - wsparcie dla IPv6
* wsparcie dla SNMP; IPMI2.0, SSH
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
* integracja z Active Directory
* możliwość obsługi przez dwóch administratorów jednocześnie
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej

Moduł wyposażony w 2 zapewniające redundancję porty RJ-45 1Gb, umożliwiający zagregowane zarządzanie wszystkimi dostarczanymi jednostkami przetwarzania. |

1. Microsoft Windows Pro 10 32/64 bit BOX USB PL (3szt)

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
| **1.** | **System operacyjny**  | Zainstalowany system operacyjny co najmniej Windows 10 Pro 64-bitowy w polskiej wersji językowej lub system równoważny wraz z nośnikiem instalacyjnym. Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu. System równoważny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.  2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim. 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.  4. Wbudowany system pomocy w języku polskim.  5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.  6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.  7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.  8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne.  9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.  10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).  14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.  15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.  16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.  18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.  20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.  22. Obsługa standardu NFC (near field communication). 23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  26. Mechanizmy logowania do domeny w oparciu o:  a. Login i hasło,  b. Karty z certyfikatami (smartcard),  c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).  27. Mechanizmy wieloelementowego uwierzytelniania.  28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.  29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.  30. Wsparcie dla algorytmów Suite B (RFC 4869). 31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.  32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.  33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.  35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 36. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.  38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.  40. Udostępnianie modemu. 41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  43. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).  44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).  45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. 46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.  48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. 49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.  |

1. **Część II: Zakup centrali telefonicznej wraz z wdrożeniem**

Szczegółowy Opis Przedmiotu Zamówienia Postępowanie „Dostawa centrali telefonicznej dla grantu Cyfrowa Gmina realizowanego przez Gminę Kiwity

Minimalne wymagania techniczne:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
| **1.** | **Telefon systemowy** | * Wbudowane 4 przyciski funkcyjne
* Wbudowany przycisk nawigacyjny
* Sygnalizacja wiadomości/dzwonka
* Haczyk do odwieszenia słuchawki
* Dwa kąty ułożenia telefonu (niski, wysoki)
* Funkcja blokady wyświetlacza oraz telefonu
* Wyświetlanie informacji o połączeniu przychodzącym
* Połączenia interkomowe lokalne lub w ramach sieci
* Wskaźnik wiadomości oczekującej
* Możliwość ustawienia różnych sygnałów dzwonienia dla różnych linii
* Funkcja oddzwaniania na zewnątrz
* Regulowane podświetlenie wyświetlacza (Automatyczny, włączony, wyłączony)
* Regulowany kontrast wyświetlacza (4 poziomy)
* Regulowana głośność słuchawki (6 poziomów)
* Regulowana głośność słuchawki nagłownej (6 poziomów)
* Regulowana głośność systemu głośnomówiącego (8 poziomów)
* Regulowana głośność dzwonka (4 poziomy, wyłączony)
* Wbudowane wejście dla słuchawki nagłownej (2.5 mm)
* Funkcja zawieszania połączeń (HOLD)
* Funkcja przekazywania połączeń (TRANSFER)
* Funkcja przekierowania połączeń: gdy zajęty, gdy nie odbiera
* Funkcja trybu nie przeszkadzaj (DND)
* Tryb automatycznego odbioru połączenia (AUTO ANSWER)
* Klawisz szybkiego zestawienia konferencji
* Wspierana obsługa słuchawek Plantronics/Jabara
* Minimum 3 liniowy LCD
 |
| **2.** | **Konsola** | * 48 przycisków o elastycznych zastosowaniach(Bezpośredni wybór stacji, programowalne, jednoprzyciskowe wybieranie numeru, często używane funkcje, sygnalizacja zajętości)
* bezpośrednie podłączenie do telefonów
* do jednego telefonu można podłączyć 4 konsole
* klawisze funkcyjne z diodami LED (zielona/
* czerwona) sygnalizującymi stan terminali
* konsolę można podłączyć za pomocą cyfrowego portu rozszerzeń,
* zamontować na stole lub ścianie oraz używać razem z terminalami cyfrowymi
 |
| **3.** | **Jednostka bazowa** | * Kolejkowanie i Inteligentna Dystrybucja Ruchu z profesjonalnymi komunikatami systemowymi i miłymi dla ucha melodiami
* Wbudowane wielokanałowe nagrywanie rozmów
* Możliwość podłączenia do czterech telefonów (w tym komórkowych) pod jednym numerem wewnętrznym
* Wideorozmowy dla dowolnej liczby użytkowników, współpraca z wideotelefonami IP, bezpłatną aplikacją dla smartfonów z systemem Android.
* współpraca z wideobramofonami IP oraz bezpłatną aplikacją dla smartfonów z systemem Android.
* Organizacja telekonferencji w pokojach konferencyjnych.
* Układ sekretarsko-dyrektorski – kierowanie przez sekretariat ruchu telefonicznego przychodzącego do dyrekcji.
* Pełna dowolność numeracji wewnętrznej i usług.
* Zdalne i lokalne zarządzanie przez przeglądarkę internetową.
* Praca w systemach Windows, Linux, Mac OS X dzięki aplikacji opartej na środowisku Java.
* Zintegrowana wewnętrzna Poczta Głosowa dla wszystkich użytkowników.
* Strefa Użytkownika dostępna przez przeglądarkę internetową.
* Zdalny dostęp dla instalatorów przez platformę.
* Obsługa wielu kart SIM – tanie rozmowy do sieci komórkowych.
* Karta I/O - moduł audio oraz sterowanie urządzeniami zewnętrznymi – automatyczne lub z dowolnego telefonu.
* Współpraca z oprogramowaniem dla call center Naso CC, dla firm taksówkarskich, z oprogramowaniem hotelowym.
* Współpraca z aplikacjami CRM, SWD, Microsoft Outlook®, typu softphone - z wykorzystaniem sterownika Platan TAPI.
* Obudowa RACK 19" do szafy teleinformatycznej.
* Gwarancja 24 miesiące
 |
| **4.** | **Sterownik centrali** | * gwarantowana obsługa 32 rozmów jednocześnie
* możliwość obsługi do 200 portów VoIP
* możliwość uruchomienia do 10 kanałów VoIP
* obsługa 1 lub 2 jednostek
* możliwość nagrywania do 16 rozmów jednocześnie
* poczta głosowa 1 godzin
* do 64 linii miejskich analogowych
* do 128 łączy ISDN BRA
* do 120 analogowych linii wewnętrznych
* do 6 portów GSM
* globalna książka telefoniczna do 3000 wpisów dla aparatów systemowych
* połączenia konferencyjne
* Inteligentna dystrybycja ruchu (infolinie – system wielopoziomowego menu głosowego, możliwość kolejkowania)
* zintegrowana wewnętrzna poczta głosowa minimum 25 kanałów
* minimum 99 zapowiedzi głosowych dla funkcji DISA oraz INFOLINII
* automatyczny wybór najtańszej drogi połączenia
* rejestracja i taryfikacja rozmów
* rozpoznawanie sygnału faksu na wszystkich liniach wewnętrznych
 |
| **5.** | **Karty wyposażenia** | * Karta wyposażenia pozwalające na podłączenie 4 jednoparowych cyfrowych aparatów systemowych i konsoli z punktu 1 oraz 2
* Karta wyposażenia ISDN BRA 2B+D (minimum 4 kanały ISDN) do centrali
* Karta wyposażenia linii miejskich analogowych do centrali – minimum 6 linii
* Karta 24 wyposażeń (podłączeń) wewnętrznych analogowych do centrali
* Karta wyposażeń w slot na kartę GSM minimum na 2 karty GSM
* Panel przyłączy krosowych
 |
| **6.** | **System zdalnego sterowania** | * Dwustopniowy system szyfrowania danych:
	+ https oraz algorytm RC4 z kluczem 256bit
* Zdalny dostęp poprzez platformę
* Licencja na nagrywanie 1 kanału centrali
* Licencja dodatkowego stanowiska odsłuchu nagrań
* Licencja na dodatkowe stanowisko nadzorcy
* Licencja na dodatkowe stanowisko administracyjne
* Licencja na stanowisko do archiwizacji nagrań
* Abonament 12 miesięcy
 |
| **7.** | **Karta SD** | * Karta microSD 4 GB z adapterem SD do nagrywania rozmów (ok. 600h) i poczty głosowej
 |
| **8.** | **Dostawa i wdrożenie** | * Wykonawca zobowiązuje się do dostarczenia, zamontowania oraz wdrożenia oferowanego sprzętu i oprogramowania, przeprowadzenia konfiguracji i integracji z istniejącą u zamawiającego infrastrukturą, dostosowanie działania centrali do wymagań zamawiającego, uruchomienie centrali. Wykonawca oświadcza, że zapoznał się z potrzebami zamawiającego w zakresie wdrożenia, konfigurowania oraz uruchomienia centrali.
* Dostawa ma zostać dokonana w dni robocze w godzinach od 7.30 do 15.00.
 |

1. **Część III: Przeprowadzenie szkolenia dla pracowników urzędu w zakresie obsługi**  **zakupionego sprzętu i oprogramowania oraz przeprowadzenie diagnozy cyberbezpieczeństwa.**

**Szkolenia stacjonarne dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania (pakiet Office 365/Microsoft 365 lub równoważne):**

1. Wstęp – ogólny opis usługi Office 365/Microsoft 365 lub równoważnego.
2. Interfejs strony głównej portal.office.com oraz dostępne aplikacje z krótkim opisem.
3. Microsoft Teams – dostępne warianty instalacji oprogramowania na różnych urządzeniach końcowych (przeglądarka, aplikacja dostępna na komputery PC/Mac, aplikacja mobilna dostępna dla smartfonów i tabletów) oraz podstawowe różnice pomiędzy wariantami.
4. Interfejs spotkania Microsoft Teams lub równoważnego oprgramowania
5. Interfejs usługi Microsoft Teams lub równoważnej :
* moduł Czat – tworzenie rozmów grupowych, wykorzystanie Czatu do rozmów audio/wideo, moduł
* kalendarz – tworzenie spotkań z uczniami, wskazanie różnic pomiędzy usługą Kalendarz dostępną w różnych aplikacjach środowiska Office 365/Microsoft 365;
* moduł Pliki – możliwe sposoby przechowywania plików w środowisku Office 365/Microsoft 365 (opis modułu realizowany z wykorzystaniem tablicy multimedialnej Microsoft Whiteboard, będącej częścią pakietu, elementy aplikacji OneDrive, Sharepoint);
* moduł Zespoły – wspólna praca nad materiałami w trakcie zajęć;
* moduł Zadania – wykonywanie zadań i testów na ocenę;
* Wykorzystywanie wzmianek oraz zabawnych rzeczy w codziennej nauce.
1. Tworzenie prezentacji multimedialnych (elementy aplikacji PowerPoint) – z wykorzystaniem aplikacji
2. PowerPoint oraz Sway.
3. Notes zajęć (aplikacja class notebook) – wykonywanie zadań w oparciu o notes zajęć.
4. Microsoft Forms lub równoważne :
* narzędzie służące do tworzenia testów sprawdzających wiedzę;
* narzędzie służące do tworzenia ankiet.
1. Cyberbezpieczeństwo:
* przykładowy scenariusz ataku hackerskiego;
* bezpieczne przechowywanie haseł;
* pojęcie mocnego hasła;
* mocne/silne uwierzytelnianie;
* wskazanie w jaki sposób można zweryfikować informacje o wyciekach własnych haseł;
* wskazanie sposobu weryfikacji siły własnego hasła.

Szkolenie - obsługa aplikacji OneNote (w tym Class Notebook oraz Staff Notebook):

1. Wstęp – ogólny opis działania oraz możliwości programu OneNote,
* różnice w wersji Class i Staff,
* efektywne wykorzystanie programu,
* aplikacja przeglądarkowa, desktopowa i mobilna.
1. Tworzenie notesu.
2. Zarządzanie notesami.
3. Możliwości notesu – dodawanie obrazu, dźwięku, tekstu, rysunków itd.
4. Sporządzanie notatek i zarządzanie nimi.
5. Wstawianie elementów (listy, łącza).
6. Formatowanie tekstu.
7. Rysunek, szkic i pismo odręczenie.
8. Wyszukiwanie notatek.
9. Wspólna praca i udostępnianie notatek.
10. Skróty klawiszowe i ułatwienie pracy.

Szkolenie - obsługa aplikacji Microsoft Word oraz Sway:

1. Wstęp – ogólny opis działania oraz możliwości aplikacji Microsoft Word oraz Sway.
2. Word:
* różnice pomiędzy aplikacją stacjonarną, a Web App;
* dodawanie, kopiowanie, edytowanie oraz formatowanie tekstu;
* modyfikacja układu stron, zmienianie marginesów, tworzenie kolumn, wstawianie nagłówków i stopek, zmiana orientacji i podziału strony;
* wstawanie tabel, obrazów, ikon, obiektów WordArt i znaków wodnych;
* zarządzanie obrazami – obracanie, zawijanie tekstu wokół;
* używanie wykresów;
* zapisywanie dokumentu, konwertowanie na format PDF, drukowanie dokumentu, etykiet i koperty.
* udostępnianie dokumentu innym użytkownikom;
* wykorzystywanie Microsoft Word w celach edukacyjnych;
* skróty klawiaturowe, narzędzia edukacyjne i korzystanie z czytnika zawartości.
1. Sway :
* jak korzystać ze sway’ów, tworzenie sway’ów przy użyciu funkcji szybki start;
* dodawanie, importowanie, osadzenie, wyszukiwanie zawartości;
* nagrywanie dźwięku;
* dodawanie więcej zawartości do sway’ów przy użyciu platformy Office 365;
* ustawienia administratora i prywatności sway’a, dodawanie haseł;
* skróty klawiaturowe;

Szkolenie - obsługa aplikacji Microsoft Excel lub równoważne:

1. Wstęp – ogólny opis działania oraz możliwości aplikacji Microsoft Excel:
* wprowadzenie do programu (wersja przeglądarkowa i aplikacja),
* menu start,
* licencje programu.
1. Tworzenie skoroszytu:
* ustawienia skoroszytu,
* opcje udostępniania, zarządzania,
* edycja komórek,
* edycja wierszy (wstawianie, edycja),
* formatowanie,
* opcje zarządzania kolorami i wyglądem.
1. Formuły, funkcje, obliczenia, skróty klawiszowe.
2. Wstawianie elementów.
3. Wykresy – tworzenie, edytowanie, typy wykresów.
4. Tabele – tworzenie, edytowanie, typy tabel.
5. Kształty – tworzenie, edytowanie, typy kształtów.
6. Współtworzenie pliku – udostępnianie, wspólna edycja.

Szkolenie – planowanie i organizacja zadań w aplikacjach Planner oraz To Do:

1. Wstęp – ogólny opis działania aplikacji Planner oraz To Do.
* możliwości wynikające z planowania wewnątrz aplikacji Planner oraz aplikacji To Do;
* powiązanie Plannera z grupami Microsoft Teams;
* dostępne aplikacje programu Planner.
1. Zarządzenie tablicą wewnątrz aplikacji Planner w tym tworzenie i modyfikacja przedziałów.
2. Dodawanie i zarządzanie zadaniami w tym:
* delegowanie zadań;
* monitorowanie postępów oraz priorytetów zadań;
* zarządzanie ramami czasowymi zadań;
* dodawanie notatek, list kontrolnych, załączników oraz komentarzy;
* tworzenie oraz wykorzystywanie etykiet;
* kopiowanie i przenoszenie zadań.
1. Analiza wykresów powiązanych z zadaniami wewnątrz aplikacji Planner.
2. Zarzadzanie harmonogramem zadań.
3. Filtrowanie i grupowanie zadań.
4. Wykorzystanie Plannera w aplikacjach Teams oraz SharePoint.
5. Zarzadzanie ustawieniami planów.
6. Eksportowanie planu do programu Excel.
7. Dodawanie planu do kalendarza Outlook.
8. Planowanie zadań z wykorzystaniem aplikacji To Do.
9. Włączanie widoczności wydelegowanych zadań w aplikacji Planner i To Do
10. Zarzadzanie oflagowanymi wiadomościami email wewnątrz aplikacji To Do
11. Tworzenie i współdzielenie list zadań z innymi użytkownikami.

Szkolenie z obsługi poczty e-mail w Outlook:

1. Wstęp – ogólny opis działania oraz możliwości programu Microsoft Outlook.
2. Dodawanie konta Outlook.
3. Opis układu i interfejsu programu.
4. Tworzenie i wysyłanie wiadomości e-mail, dodawanie podpisów i załączników.
5. Zarządzanie pocztą email:
* konfiguracja automatycznych odpowiedzi;
* oczyszczanie skrzynki pocztowej;
* ignorowanie wiadomości;
* wyszukiwanie i filtrowanie wiadomości.
1. Konfigurowanie flag, kategorii, przypomnień, kolorów oraz reguł.
2. Kontakty i zadania:
* dodawanie kontaktów;
* tworzenie grupy kontaktów;
* importowanie/eksportowanie kontaktów;
* tworzenie listy zadań.
1. Kalendarz:
* tworzenie terminów i spotkań;
* udostępnianie/importowanie kalendarza;
* planowanie spotkania online z wykorzystaniem aplikacji Teams.
1. Obsługa Outlook w sieci Web:
* wprowadzenie do aplikacji Outlook Web App;
* praca w trybie offline;
* tworzenie nowego folderu;
* otwieranie i używanie udostępnionej skrzynki pocztowej w aplikacji Outlook w sieci Web.

Szkolenie – administracja tożsamościami Azure Active Directory:

1. Wstęp:
* czym jest Azure;
* czym jest Active Directory;
* jak rozumieć pojęcie tożsamości wewnątrz pakietu Office 365/Microsoft 365.
1. Użytkownicy:
* tworzenie i zarządzanie użytkownikami wewnątrz Azure Active Director;
* wykonywanie operacji zbiorczych na użytkownikach;
* resetowanie haseł;
* włączanie samoobsługowego resetowania haseł;
* zarzadzanie ustawieniami użytkownika;
* przeglądanie logów powiązanych z użytkownikami;
* przeglądanie dziennika inspekcji;
* modyfikacja parametrów użytkownika;
* zrządzanie rolami użytkownika, członkostwa w grupach;
* zarzadzanie licencjami użytkownika w Azure Active Director;
* opis zasadności wykorzystania rozwiązań typu MDM, czyli Mobile Device Management;
* diagnozowanie i rozwiązywanie problemów.
1. Zarządzanie grupami:
* ustawienia i zasady grup;
* wykorzystanie dziennika inspekcji względem grup;
* modyfikacja parametrów grup oraz wyjaśnienie zasady propagacji zmian grup w aplikacjach pomiędzy tradycyjnym panelem administracyjnym Azure Active Director, aplikacjami Outlook, SharePoint oraz Teams;
* zarządzanie członkami grup.
* Zarządzanie zespołami oraz zasady zespołów i konfiguracja zasad zespołów.
* Zarządzanie fizycznymi urządzeniami służącymi do obsługi kont Microsoft Teams takimi jak – telefony, IP.
* Zarządzanie lokalizacjami, w tym topologia sieci.
* Zarządzanie użytkownikami, w tym analiza historii rozmów i rozwiązywanie problemów technicznych użytkowników oraz generowanie raportów powiązanych z użytkownikami.
* Zarządzanie spotkaniami oraz zdarzeniami na żywo. Konfiguracja zasad i ustawień spotkań oraz zdarzeń na żywo.
* Zasady obsługi wiadomości typu chat.
* Zarządzanie dostępem do aplikacji firm trzecich oraz konfiguracja zasad uprawnień.
* Konfiguracja pakietów zasad.
* Obsługa raportów oraz analiz, w tym generowanie raportów użytkowania aplikacji przez uczniów i nauczycieli, które mogą być wykorzystane np. przez dyrekcje szkoły.
* Zarządzanie zadaniami przydzielanymi w ramach platformy Teams.
* Globalne ustawienia całej organizacji.
* Wykorzystanie planowania oraz doradcy aplikacji Teams.
* Obsługa panelu jakości rozmów.

**Szkolenie z zakresu cyberbezpieczeństwa dla pracowników Zamawiającego oraz konsultacje w zakresie doskonalenia, monitorowania i wdrożenia zmian w systemie zarządzania bezpieczeństwem informacji w ramach realizacji Projektu Cyfrowa Gmina.**

**Etap I - Audyt przedwdrożeniowy**

**Zamawiający wskazuje, iż równoważne z przeprowadzeniem audytu przedwdrożeniowego jest przeprowadzenie u Zamawiającego wstępnej diagnozy cyberbezpieczeństwa w oparciu o załącznik nr 8 do Regulaminu Konkursu Cyfrowa Gmina.**

1. Weryfikacja poziomu spełnienia wymagań określonych w rozporządzeniu w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów

teleinformatycznych Krajowych Ram Interoperacyjności, w tym ocenę skuteczności

zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych u Zamawiającego.

2. Wykonawca zbada zgodność działań Zamawiającego z uregulowaniami prawnymi.

3. Audyt podlega przeprowadzeniu we wszystkich komórkach organizacyjnych jednostki

4. Przed rozpoczęciem prac Wykonawca przedstawi Zamawiającemu do akceptacji plan audytu.

5. Zakres prac audytu przedwdrożeniowego będzie obejmował co najmniej:

· zapoznanie się ze strukturą organizacyjną Zamawiającego;

· analizę i ocenę dokumentacji wewnętrznej, które Zamawiający udostępni Wykonawcy do analizy;

· wywiady analityczne z wyznaczonymi przez Zamawiającego pracownikami komórek

· organizacyjnych w zakresie niezbędnym do ustalenia poziomu stosowania wymagań

· bezpieczeństwa określonych w Krajowych Ram Interoperacyjności i wewnętrznych uregulowaniach Zamawiającego;

· analizę bezpieczeństwa zasobów teleinformatycznych Zamawiającego

6. Wykonawca opracuje i sporządzi raport z przeprowadzonego audytu przedwdrożeniowego, zawierający w szczególności:

· cel i zakres audytu;

· szczegółowy opis przeprowadzonych prac;

· opis poziomu spełnienia każdego z wymagań bezpieczeństwa określonych w Krajowych Ramach Interoperacyjności;

· wykaz stwierdzonych niezgodności i rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności w odniesieniu do każdego z wymagań określonych w Krajowych Ramach Interoperacyjności;

· podsumowanie i wnioski.

7. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu. Wykonawca zobowiązany jest do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego.

**Etap II - Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji**

**i Polityki Bezpieczeństwa Informacji**

1. Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu

2. przedwdrożeniowego, zobowiązany jest zaproponować organizację Systemu Zarządzania Bezpieczeństwem Informacji oraz opracować i przedstawić koncepcję wdrożenia Polityki Bezpieczeństwa Informacji u Zamawiającego.

3. Koncepcja będzie w szczególności zawierać mapę dokumentów, stanowiącą szczegółowy

4. wykaz dokumentów z zaznaczeniem ich wzajemnych powiązań, w tym:

a) Dokument Główny Polityki Bezpieczeństwa Informacji definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa w proces zapewnienia bezpieczeństwa informacji, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji;

b) Polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji u Zamawiającego w tym dla obszaru: teleinformatycznego, spraw osobowych, zabezpieczeń fizycznych, ciągłości działania, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa;

c) Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

5. Zamawiający zastrzega sobie prawo do wnoszenia uwag do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego. Uwagi wniesione przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji wdrożenia SZBI i PBI.

6. Na podstawie zatwierdzonej przez Zamawiającego koncepcji Wykonawca opracuje wszystkie opisane w koncepcji dokumenty. Dokumenty muszą być zgodne ze wszystkimi wymaganiami prawnymi, którym podlega Zamawiający. Jeżeli w czasie realizacji umowy wymagania prawne w zakresie bezpieczeństwa informacji ulegną zmianie, Wykonawca zobowiązany jest dostosować dokumentację PBI do zaistniałych zmian.

7. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego.

**Etap III - Szkolenia z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki**

**Bezpieczeństwa Informacji oraz cyberbezpieczeństwa**

Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji oraz cyberbezpieczeństwa dla wszystkich pracowników Zamawiającego, obejmujących co najmniej:

a) omówienie podstawowych zasad bezpieczeństwa informacji, wynikających z SZBI i PBI;

b) odpowiedzialność za naruszenie zasad SZBI i PBI;

c) zasady zgłaszania i reagowania na incydenty

d) bezpieczeństwo informatyczne w miejscu pracy.

Szkolenia dla pracowników zostaną przeprowadzone w formie stacjonarnej lub on-line;

szkolenie każdej grupy będzie obejmować 6 godzin w czasie jednego dnia szkolenia.

Zamawiający zastrzega sobie prawo do rejestracji audiowizualnej przebiegu szkoleń.

**Szczegółowy opis wymagań diagnozy cyberbezpieczeństwa:**

**I. Informacje ogólne Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu diagnozy cyberbezpieczeństwa u Zamawiającego zgodnie z wymogami Programu Operacyjnego Polska Cyfrowa na lata 2014 –2020 Działanie 5.1 Rozwój cyfrowy JST, pod kątem rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI) oraz w oparciu o normę PN-ISO/IEC 27001 standaryzującą systemy zarządzania bezpieczeństwem informacji.**

Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

W ramach Zadania Wykonawca przeprowadzi audyt (diagnostyczny) funkcjonującego u Zamawiającego Systemu Zarządzania Bezpieczeństwem Informacji pod względem zgodności z następującymi aktami prawnymi oraz normami:

1. ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070, z późn. zm.) (w zakresie dotyczącym bezpieczeństwa informacji), 2. rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) (w zakresie dotyczącym bezpieczeństwa informacji),

2. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

3. ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560),

4. aktualne normy PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 27701, PNISO/IEC 27017 oraz PN-ISO/IEC 22301.

Podstawę audytu będą stanowiły, co najmniej:

1. wywiady z przedstawicielami Zamawiającego

2. obserwacje lub wywiady audytora, dotyczące bezpieczeństwa fizycznego i środowiskowego,

3. obserwacje lub wywiady audytora, dotyczące bezpieczeństwa serwerowni,

4. obserwacje lub wywiady audytora dotyczące bezpieczeństwa kluczowych systemów teleinformatycznych,

5. zgromadzone materiały audytowe w postaci dokumentacji bezpieczeństwa informacji i organizacyjnej obowiązującej u Zamawiającego.

Usługa ma być przeprowadzona w siedzibie Zmawiającego (Zamawiający informuje, iż dopuści wykonywanie prac w sposób zdalny w zakresie, w jakim osobista obecność Wykonawcy nie jest konieczna oraz umożliwi Wykonawcy dostęp do użytkowników i infrastruktury technicznej za pośrednictwem łącz komunikacji zdalnej)

Efektem realizacji Zadania I będzie raport z przeprowadzonego audytu bezpieczeństwa, przygotowany i przekazany Zamawiającemu w formie elektronicznej.

Raport będzie zawierał co najmniej:

1. opis wykonania planu audytu,

2. opis wykorzystanych standardów,

3. ocenę spełnienia wymagań.

**II. Szczegółowy Zakres Audytu W ramach zamówienia, Wykonawca przeprowadzi diagnozę na podstawie następujących obszarów i dokumentów:**

Identyfikacja systemu informacyjnego wspierającego zadanie publiczne;

* Dokumentacja dot. zarządzania incydentem,
* Dokumentacja dot. wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa,
* Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji,
* Regulacje wewnętrzne dot. zmieniającego się otoczenia,
* Inwentaryzacja sprzętu i oprogramowania,
* Analiza ryzyka utraty integralności, dostępności lub poufności informacji, postępowanie ryzykiem,
* Dokumentacja dot. zarządzania uprawnieniami,
* Dokumentacja dot. szkoleń i uświadamiania,
* Dokumentacja dot. monitorowania dostępu do informacji, nieautoryzowanych zmian i zabezpieczenia nieautoryzowanego dostępu,
* Zasady bezpiecznej pracy mobilnej,
* Dokumentacja dot. zabezpieczenia informacji przed nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem,
* Umowy serwisowe,
* Zasady postępowania z informacjami w celu minimalizacji ryzyka kradzieży,
* Dokumentacja dot. zapewnienia odpowiedniego poziomu bezpieczeństwa (w tym oprogramowania, utraty w wyniku awarii, ochrony przed błędami, mechanizmów kryptograficznych, bezpieczeństwa plików, zarządzania podatnościami, kontroli zgodności z regulacjami),
* Dokumentacja dot. audytu bezpieczeństwa informacji, System informacyjny wspierający zadanie publiczne;
* Raport z audytu systemu informacyjnego,
* Dokumentacja architektury zastosowanych zabezpieczeń,
* Dokumentacja architektury sieci,
* Baza danych konfiguracji urządzeń aktywnych,
* Dokumentacja zmian w systemach informacyjnych,
* Dokumentacja dot. monitorowania w trybie ciągłym,
* Umowy z dostawcami wsparcia technicznego,
* Umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego,
* Raport z audytu dostawcy usług teleinformatycznych,
* Dokumentacja zabezpieczeń fizycznych i środowiskowych,
* Rejestr dostępu do dokumentacji systemu informacyjnego,

Aspekty techniczne;

* Raport z audytu serwisu WWW,
* Raport z audytu serwisu pocztowego,
* Raport z audytu lokalnych sieci teleinformatycznych,
* Raport z audytu połączenia z siecią Internet Aspekty organizacyjne;

Aspekty organizacyjne:

* Raport z audytu organizacji zarządzania bezpieczeństwem teleinformatycznym,
* Raport z audytu procesu planowania,