Załącznik nr 1

Szczegółowy opis przedmiotu zamówienia

kwiecień 2022

1 Spis treści

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

- całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
- całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

2. Wymagania gwarancyjne.

Sprzęt

- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. roczna gwarancja (chyba, że zapisy szczegółowe stanowią inaczej) oparta na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
- Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
- Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;
- wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń sieciowych i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

3. Miejsce instalacji sprzętu i oprogramowania/systemu.

- Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części załącznika na 1, w budynkach urzędu w miejscach wskazanych przez Zamawiającego.

4. Ubezpieczenie sprzętu

Wykonawca zobowiązany jest do dostawy sprzętu komputerowego wraz z ubezpieczeniem na okres 12 m-cy. Koszty ubezpieczenia należy ująć w cenie oferowanego sprzętu.
Sprzęt musi zostać ubezpieczony do 100% jego wartości księgowej brutto.
Ubezpieczenie nie może przewidywać franszyzy, integralnej i udziału własnego ze strony Zamawiającego.
Polisa ubezpieczeniowa powinna zostać wystawiona na rzecz Zamawiającego.
Dostarczony sprzęt powinien zostać objęty ubezpieczeniem od wszelkich ryzyk zgodnie z poniższymi założeniami:

1. Przedmiotem ubezpieczenia jest sprzęt elektroniczny stacjonarny zainstalowany na stałe w miejscu ubezpieczenia oraz sprzęt przenośny, pod warunkiem, że wiek sprzętu elektronicznego stacjonarnego i sprzętu przenośnego nie przekracza 5 lat.
2. Sprzęt przenośny używany poza lokalem na terenie Rzeczypospolitej Polskiej jest objęty ochroną w przypadku jego utraty wskutek kradzieży z włamaniem, jeżeli został skradziony z samochodu, gdy:
   a. pojazd posiadał twardy dach (jednolitą sztywną konstrukcję),
   b. został prawidłowo zamknięty na wszystkie możliwe zabezpieczenia znajdujące się w pojeździe,
   c. był zaparkowany w zamkniętym garażu lub na parkingu strzeżonym (jeżeli kradzież z włamaniem nastąpiła w godzinach 22.00 - 6.00),
   d. ubezpieczony przedmiot był przechowywany wewnątrz pojazdu w sposób uniemożliwiający zobaczenie go z zewnątrz, np. w bagażniku.
3. Zakres ubezpieczenia:
   1) Od wszystkich ryzyk z rozszerzeniem o użytkowanie mobilne w tym m.in.:
      a. utrata bądź ubytek wartości ubezpieczonego sprzętu nastąpiły z powodu jego zniszczenia lub uszkodzenia w wyniku nieprzewidzianego wypadku uniemożliwiającego dalsze spełnianie zamierzonych funkcji.
      b. utrata sprzętu nastąpiła wskutek kradzieży z włamaniem, rabunku, dewastacji i wandalizmu.
   2) Do szkód objętych ubezpieczeniem zalicza się m.in. szkody wynikłe w następstwie:
      a. działania człowieka:
         a. niewłaściwej obsługi sprzętu, tj. nieostrożności, zaniedbania, niewłaściwego użytkowania,
         b. braku kwalifikacji, błędu operatora itp.;
         c. świadomego i celowego zniszczenia przez osoby trzecie, pracowników i współpracowników ubezpieczającego (jednak z zastosowaniem klauzuli reprezentantów),
      b. kradzieży z włamaniem, rabunku, wandalizmu i dewastacji. Ubezpieczyciel ponosi odpowiedzialność także za szkody powstałe wskutek kradzieży z pojazdu lub kradzieży całego pojazdu wraz ze sprzętem.
      c. ognia (w tym działania dymu, sadzy itp.) oraz polegające na osmaleniu, przypaleniu, a także w wyniku wszelkiego rodzaju eksplozji, implozji, uderzenia piorunu bezpośrednio i pośrednio na przedmiot ubezpieczenia, upadku statku powietrznego oraz w akcji ratunkowej
      d. wody, tj. zalania wodą z urządzeń wodno – kanalizacyjnych, powodzi, wylewu wód podziemnych, a także czynników atmosferycznych w postaci mrozu, śniegu, deszczu wilgoci, pary wodnej itp.
      e. wiatru, gradu, lawiny, obsunięcia i zapadania się ziemi, huraganu, trzęsienia ziemi,
      f. zbyt wysokiego lub zbyt niskiego napięcia albo całkowitego zaniku napięcia w sieci instalacji elektrycznej, szkód przepięciowych i pochodnych powstałych w związku z uderzeniem pioruna,
      g. sprzęt elektroniczny ubezpieczony jest również w zakresie szkód spowodowanych przez upadek.
   3) Dodatkowe rozszerzenie dotyczące ochrony sprzętu nie podłączonego na stanowisku pracy lub podczas przerwy w eksploatacji.

5. Zestawienie zakresu dostaw i usług.

Lp.	Nazwa	Długość gwarancji (minimum) [m-ce]	Ilość	Jednostka miary	Uwagi

1.	Serwer	12 (kryterium oceny)	1	Szt.	Zamawiający obecnie posiada przestarzałe serwery poza okresem gwarancji. Konieczny jest zakup nowego serwera wyposażonego w dużą ilość pamięci RAM i zasób dyskowy. Urządzenie posłuży jako podstawa do wirtualizacji kolejnych maszyn oraz miejsce składowania danych dla systemów dziedzinowych. Parametry: 2 procesory 8 corowe, min. 256 GB RAM, HDD: 6xSATA min. 6TB + 6xSSD min. 1,92TB, 2xzasilacz.
2.	System Backupu - NAS	12 (kryterium oceny)	1	Szt.	System NAS posłuży jako miejsce przechowywania kopii zapasowych. System będzie wyposażony we własne oprogramowanie do tworzenia kopii zapasowych i bezpieczeństwa oraz w min. 6 dysków HDD 6TB każdy
3.	Switch	12 (kryterium oceny)	2	Szt.	Pozycja uwzględnia koszt zakupu 2 przełączników sieciowych 24 portowych o przepustowości min. 1Gb z portami uplink 10G. Urządzenia pozwolą na dołączenie lokalnych zasobów komputerowych do sieci LAN
4.	Firewall	12 (kryterium oceny)	1	Szt.	W pozycji zaplanowano zakup urządzenia UTM służącego do zabezpieczenia i zarządzania ruchem w całej sieci LAN wraz z podłączeniem łącza internetowego. Urządzenie zapewni również możliwość pracy zdalnej poprzez dedykowane, szyfrowane kanały VPN zestawiane na publicznej sieci internet oraz publikację e-usług.
5.	UPS	12 (kryterium oceny)	1	Szt.	Urządzenie pozwoli na podłączenie zakupionych urządzeń w bezpieczny sposób do sieci elektrycznej zapewniając właściwe warunki pracy w momencie braku zasilania. Zwiększy poziom bezpieczeństwa przechowywanych danych, eliminując zagrożenie utarty danych w wyniku niewłaściwego, nagłego wyłączenia urządzeń.
6.	Oprogramowanie do wirtualizacji	12 (kryterium oceny)	1	Szt.	Oprogramowanie do wirtualizacji niezbędne do uruchomienia maszyn wirtualnych na zakupionym serwerze. Oprogramowanie konieczne do zapewnienia warunków pracy zdalnej i

					świadczenia e-usług publicznych przez gminę.
7.	Domena	wieczysta	1	Szt.	Kalkulacja pozycji uwzględnia koszty systemu operacyjnego niezbędnego do funkcjonowania serwerów wirtualizacji i backupu oraz koszty licencji dostępowych (CAL) dla użytkowników (50 licencji). Zakup jest niezbędny do zapewnienia dostępu i funkcjonowania całej planowanej infrastruktury.
8.	Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania - Instalacja i konfiguracja	12	1	Szt.	Kalkulacja obejmuje koszty usług doradczych związanych z wdrożeniem platformy sprzętowej (wirtualizacyjnej), migracją danych z dotychczasowych urządzeń, ustaleniem i skonfigurowaniem zasad bezpieczeństwa sieciowego, montaż urządzeń, instruktaż z zakresu wdrożonych rozwiązań dla służb informatycznych w urzędzie. Dla całości usług przewidziano 75 godz., Zakres usługi: ○ Instalację i konfiguracje zakupionych urządzeń. ○ Migrację danych ze starych maszyn na nowy serwer. ○ Instalację i konfiguracje domeny. ○ Opracowanie polityk bezpieczeństwa sieci, założenie kont użytkowników. ○ Instruktaż dla służb informatycznych. ○ Wsparcie techniczne, nadzór autorski 12 miesięcy.
9.	Diagnoza cyberbezpieczeństwa	12	1	Szt.	Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina",

5.1. Serwer – szt. 1 – wymagania minimalne.

Lp.	Parametr	Wymagania minimalne
1.	Obudowa	• Typu RACK, wysokość nie więcej niż 2U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
2.	Płyta główna	• Dwuprocesorowa; • Wyprodukowana i zaprojektowana przez producenta serwera • 6 złącz PCI Express generacji 3 w tym: • 3 złącza o prędkości x16 • 3 złącza o prędkości x8 • 12 gniazd pamięci RAM; • Obsługa minimum 768GB pamięci RAM; • Możliwość zainstalowania modułu TPM;

		• Wsparcie dla technologii: • Memory Scrubbing • SDDC • Advanced ECC
3.	Procesory	• Dwa procesory 8-rdzeniowe • architektura x86_64 • Taktowanie bazowe 3,2GHz zapewniający wydajność min. 15000 pkt. (dla pojedynczego procesora) w teście Passmark CPU Mark, znajdujący się na liście https://www.cpubenchmark.net/cpu_list.php (wynik na dzień 08.02.2021)
4.	Pamięć RAM	• 256 GB pamięci RAM • DDR4 Registered • 2933Mhz
5.	Dyski twarde	• Minimum 12 wnęk dla dysków twardych Hotplug 3,5"; • Zainstalowane 6 dysków SSD SATA 1,92TB HOT PLUG 3.5" • Zainstalowane 6 dysków HDD SATA 6TB HOT PLUG
6.	Kontrolery LAN	• Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI i iSCSI boot; • Dodatkowa karta 2x 10Gbit SFP6
7.	Kontrolery I/O	• Kontroler RAID dla wewnętrznych dysków twardych posiadający obsługujący poziomy RAID: 0,1,10,5,50,6,60 posiadający 2GB pamięci cache, zabezpieczonej przed utratą danych w przypadku awarii zasilania (FBU lub BBU)
8.	Porty	• Zintegrowana karta graficzna ze złączem VGA; • 1 porty USB na panelu przednim; • 1 port USB 3.0 wewnętrzny; • 4 porty USB 3.0 dostępne z tyłu serwera; • 1 port serial/RS232 – możliwość rozbudowy; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;
9.	Zasilanie, chłodzenie	• Dwa zasilacze hotplug o sprawności 94% (tzw klasa Platinum) o mocy 800W, redundancja zasilania; • Redundantne wentylatory;
10.	Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera; • Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web, SSH; • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej

		• Możliwość zarządzania przez 6 administratorów jednocześnie • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) - funkcjonalność aktywna dożywotnio, bez żadnych ograniczeń; • Obsługa serwerów proxy (autentykacja) • Obsługa VLAN • Możliwość konfiguracji parametru Max. Transmission Unit (MTU) • Wsparcie dla protokołu SSDP • Obsługa protokołów TLS 1.2, SSL v3 • Obsługa protokołu LDAP • Integracja z HP SIM • Synchronizacja czasu poprzez protokół NTP • Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); • Wbudowana w kartę zarządzającą (lub zainstalowana) pamięc flash o pojemności minimum 16 GB; Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
11.	Wspierane OS	• Microsoft Windows Server 2019, 2016 • VMWare vSphere 6.7, 7.0 • Suse Linux Enterprise Server 12, 15 • Red Hat Enterprise Linux 7, 8
12.	Gwarancja	• 3 lata gwarancji producenta serwera w trybie onsite z gwarantowaną skuteczną naprawa do końca następnego dnia roboczego; • Dyski twarde nie podlegają zwrotowi organizacji serwisowej; • Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu (bez udziału administratora); • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);

13.	Dokumentacja, inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy; • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

5.2. Backup NAS – szt. 1 – wymagania minimalne

- Procesor osiągający w teściem CPU Mark na stronie https://www.cpubenchmark.net/cpu_list.php wartość min. 5200 punktów
- Prędkość odczytu, min. 450.00 MB/sek
- Prędkość zapisu min. 450.00 MB/sek
- Wbudowany interfejs 1Gbit/s z min. czterema portami RJ-45 oraz funkcją agregacji łączy
- Możliwość zainstalowania karty SSD M.2 lub 10GbE
- Pamięć RAM min. 4GB (możliwość rozbudowy do min. 32 GB w min 2 slotach)
- Ilość kieszeni dysków min. 8 (możliwość rozbudowy do 12 dysków z wykorzystaniem jednostki rozszerzającej lub równoważnie obudowa na 12 dysków)
- Obudowa 19 cali max. 2U z szynami do montaży w szafie teleinformatycznej
- Port USB 3.0 min. 2 szt.
- Port eSATA min 1 szt.
- Obsługiwane typy dysków:
  - 3,5” SATA HDD
  - 2,5” SATA HDD
  - 2,5” SATA SSD
- Obsługiwany poziom RAID:
  - Basic
  - JBOD
  - RAID 0
  - RAID 1
  - RAID 10
  - RAID 5
  - RAID 6
- Urządzenie musi zostać dostarczone z min. 6 szt. dysków twardych o pojemności min 6TB.
- Wsparcie dla środowisk wirtualizacji takich jak VMware, Citrix oraz Microsoft Hyper-V.
- Wbudowany serwer FTP z funkcjami SSL, TLS.
- Obsługa Windows AD, LDAP oraz Domain Trust.
- Ochrona za pomocą funkcji kopii zapasowych, jednostek LUN, migawek, klonowania i synchronizacji danych.
- Panel użytkownika i oprogramowanie dostępne w pełnej polskiej wersji językowej.
- Wbudowane systemy zabezpieczeń sieciowych, antywirus, szyfrowanie AES256bit oraz dwustopniowe uwierzytelnianie użytkowników.

- Urządzenie musi być wyposażone w zintegrowane rozwiązanie do tworzenia kopii zapasowych dla serwerów fizycznych z systemem Windows/Linus, komputerów z systemem Windows, serwerów plików rsync/SMB oraz maszyn wirtualnych VMware vSphere/Microsoft Hyper-V.
- Urządzenie musi posiadać centralny interfejs zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, zużycia pamięci masowej i transmisji danych historycznych.
- Oprogramowanie do backupu musi umożliwiać szybkie przywracanie plików, całych maszyn fizycznych i maszyn wirtualnych.

5.3. Switch - szt. 2 – wymagania minimalne

Urządzenia sieciowe i osprzęt sieciowy pozwalający na przyłączenie do szerokopasmowego Internetu.
Przełącznik wielowarstwowy L2/L3, zarządzany

Typ i liczba portów:

Min. 24 porty 10/100/1000BaseT RJ-45, min. uplink 4x10G SFP+

Porty SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:

- Gigabit Ethernet 1000Base-SX
- Gigabit Ethernet 1000Base-LX/LH
- 10Gigabit Ethernet 10GBase-SR
- 10Gigabit Ethernet 10GBase-LR
- 10Gigabit Ethernet typu twinax

Port konsoli USB Type-B/RJ45

Porty dostępowe przełącznika musza być zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

Parametry wydajnościowe:

- Przepustowość przełącznika (switching bandwidth) min. 125 Gb/s
- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów min. 95 Mpps
- Pamięć DRAM – min. 512 MB
- Pamięć flash – min. 256 MB
- Wielkość bufora pakietów – min. 1,5 MB
- Min. 255 grup IGMP
- Min. 4 grupy połączeń zagregowanych typu „port channel” LACP
- Min. 8 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
- Min. 512 wpisów w listach kontroli dostępu ACL
- Min. 8 kolejek sprzętowych

Obsługa:

- Min. 255 aktywnych sieci VLAN
- Min. 8 000 adresów MAC
- Min. 32 statyczne trasy IPv4
- Min. 16 interfejsów L3
- ramek Ethernet Jumbo 9 000 B

Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

- IEEE 802.1w Rapid Spanning Tree
- Per-VLAN Rapid Spanning Tree (PVRST+)
- IEEE 802.1s Multi-Instance Spanning Tree
- Obsługa 126 instancji protokołu STP

Przełącznik musi wspierać:

- obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
- protokół rejestracji GARP VLAN (GVRP)

Przełącznik musi wspierać mechanizmy związane z bezpieczeństwem sieci:

- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
- Autoryzacja użytkowników w oparciu o IEEE 802.1X
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
- Obsługa HTTPS, SSH, SSL,
- Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP)

Przełącznik musi wspierać mechanizmy związane z zapewnieniem jakości usług w sieci:

- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
- Implementacja algorytmu Weighted Round Robin dla obsługi kolejek
- Możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi,
- Kontrola sztormów dla ruchu broadcast/multicast/unicast
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

Przełącznik musi wspierać obsługiwać standardy komunikacyjne:

IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet

Obsługa protokołu NTP
Funkcje DHCP server, DHCP relay
Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snooping
Blokowanie Head of Line (HOL)

Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD)
Zapobieganie atakom DoS

Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6

Zarządzanie

- Port konsoli
- Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
- Obsługa protokołów SNMPv3, SSHv2, https, syslog
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia
- Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki

- Obsługa protokołu LLDP i LLDP-MED
- Obsługa funkcji Plug & Play
- Przycisk reset

Inne

- Zasilanie 230V AC
- Wysokość maksymalnie 1U, montowany w szafie typu RAC 19''
- Wraz z przełącznikami należy dostarczyć 8 szt. kabli DAC o przepustowości 10G SFP+

5.4. Firewall - szt. 1 – wymagania minimalne

Wymagania Ogólne

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, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB.
5. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe 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.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. 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.

5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. 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.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. 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.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

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

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

5.5. UPS – szt.1 – wymagania minimalne.

Lp.	Parametr	Opis funkcjonalności
1	Minimalne wymagania techniczne	• Moc znamionowa jednostki nie mniej niż 5000VA / 4500W • Jednostka do montażu w szafie Rack(szyny montażowe w zestawie) • Technologia podwójnej konwersji (online) • Temperatura eksploatacji 0 - 40 °C • Klasa ochrony IP 20
2	Parametry wejściowe	• Nominalne napięcie wejściowe 230V_{AC} • Częstotliwość wejściowa 40–70 Hz (wykrywanie automatyczne) • Typ gniazda wejściowego: - Hard Wire 3 wire (1PH+N+G)
3	Parametry wyjściowe	• Napięcie wyjściowe 230VAC • Zniekształcenia napięcia wyjściowego <2% • Częstotliwość na wyjściu 50/60Hz ±3 Hz • Inne napięcia wyjściowe 220, 240 • Współczynnik szczytu 3: 1 • Typ przebiegu sinusoida • Złącza/gniazda wyjściowe (6) IEC 320 C13 (Zasilanie gwarantowane) (4) IEC 320 C19 (Zasilanie gwarantowane) • Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)
4	Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu • Czas autonomii: ≥ 4 minuty dla pełnego obciążenia ≥ 11,5 minuty dla połowy obciążenia • Typowy czas ładowania ≤1,5 godziny • Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów • Baterie wymieniane na gorąco
5	Komunikacja i zarządzanie	• Puste gniazdo do montażu dodatkowej karty np. WEB/SNMP • Port do podłączenia np. czujnika temperatury • Porty komunikacyjne: RJ45 Serial, RJ45 SNMP, USB • Panel sterowania z wyświetlaczem LCD • Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia • Awaryjny wyłącznik zasilania (EPO)

		• Oprogramowanie do zamykania systemów operacyjnych

5.6. Oprogramowanie do wirtualizacji – szt.1 – wymagania minimalne.

Licencja dla dostarczonego serwera fizycznych posiadającego 2 procesory z gwarancją utrzymania aktualnej wersji przez okres min. 1 roku,

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć
5. i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
7. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych
9. z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM.
10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
11. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
12. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
13. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
14. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami.
15. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2012, Windows Server 2019, Windows Server 2022, Windows 10, Windows 11, SLES, RHEL, Solaris, OS/2, NetWare, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu SCO OpenServer, SCO Unixware, Mac OS X.
16. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
17. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
18. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.
19. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
20. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
21. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
22. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
23. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.

24. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
25. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
26. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
27. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych.
28. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
29. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
30. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

5.7. Domena – szt. 1 – wymagania minimalne.

Licencje na serwerowy system operacyjny – szt. 2

Licencje na serwerowy system operacyjny muszą uprawniać do zainstalowania serwerowego systemu operacyjnego 2 oferowanych serwerach fizycznych lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego na każdym z 2 oferowanych serwerów fizycznych. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanych serwerach.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18) Mechanizmy logowania w oparciu o:
    a) Login i hasło,
    b) Karty z certyfikatami (smartcard),
    c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) 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:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c) Zdalna dystrybucja oprogramowania na stacje robocze.

d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   i. Dystrybucję certyfikatów poprzez http
   ii. Konsolidację CA dla wielu lasów domeny,
   iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f) Szyfrowanie plików i folderów.
g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i) Serwis udostępniania stron WWW.
j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
k) Wsparcie dla algorytmów Suite B (RFC 4869),
l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
   i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   iii. Obsługi 4-KB sektorów dysków
   iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
26) 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.
27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Licencje dostępowe:
Wymaga się aby oferowane licencje dla systemu operacyjnego umożliwiały korzystanie z zasobów dla 50 użytkowników (50 licencji dostępowych).

5.8. Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania

Instalacja i konfiguracja

1.	**Usługi**	Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji e-usług publicznych, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. Część sprzętowa powinna zostać oparta na systemie wirtualizacji zasobów IT. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. **W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową**. Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym: a) Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia. b) Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności: i. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych. ii. schematy połączeń iii. mechanizmy działania głównych elementów sprzętowych: • sieć LAN • system wirtualizacyjny • system backupu i archiwizacji danych • system serwerowy • Firewall/UTM iv. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności v. sposób odbioru uzgodniony z Zamawiającym vi. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu vii. opis przypadków, w których projekt dopuszcza niedziałanie systemu viii. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą

		Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia.
2.	**Montaż i fizyczne uruchomienie systemu**	**Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:** 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. 2. Urządzenia, które nie są montowane w szafach teleinformatycznych powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 3. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 4. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 5. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 6. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 7. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 8. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). 9. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem: a. Stworzenia połączeń sieci LAN pomiędzy przełącznikami. b. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN. c. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1. d. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
3.	**Instalacja i konfiguracja oprogramowania**	1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. 2. Instalacja i konfiguracja dostarczonego oprogramowania do systemu wykonywania backupu i archiwizacji danych. 3. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego).

		4. Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych.
4.	**Konfiguracja przełączników sieci LAN:**	Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi lokalizacjami występującymi w projekcie według topologii gwiazdy. Centralnym punktem będzie serwerownia zlokalizowana w Urzędzie. Przełączniki będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego). Konfiguracja dostarczanych przełączników w zakresie: a. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. b. Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów. c. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym). d. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN. i. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink. ii. Z wykorzystaniem połączeń światłowodowych oraz miedzianych. iii. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu. iv. Należy wykorzystać wkładki o najwyższej możliwej przepustowości dla danego połączenia np.: dla portu o możliwej przepustowości 1/10Gbs (wkładka: SFP/SFP+), należy wykorzystać wkładki SFP+ o przepustowości 10Gbps. e. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN. f. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster; g. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK). h. Ustawienie serwera czasu dla urządzeń sieci LAN – przełączników sieciowych - na firewall. i. Zamawiający wymaga instalacji i konfiguracji serwera logów dla urządzeń sieci LAN (maszyna wirtualna) – przełączników sieciowych, z graficznym interfejsem przeszukiwania. Zamawiający dopuszcza rozwiązania Open Source. j. Zamawiający wymaga instalacji i konfiguracji dedykowanego serwera monitorowania pracy urządzeń sieciowych z graficznym interfejsem przeszukiwania (maszyna wirtualna): przełączniki sieciowe, drukarki, UTM. Zamawiający dopuszcza rozwiązania Open Source. k. Wykonawcza skonfiguruje urządzenia aby raportowały, przesyłały dane do zainstalowanego serwera logów i monitorowania sieci. l. Testowanie obsługi ruchu sieciowego. m. Testowanie skuteczności zabezpieczeń.

5.	**Konfiguracja elementów bezpieczeństwa sieciowego.**	Urządzenie firewall/modernizacja konfiguracji urządzenia UTM w zakresie. 1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta. 3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu. 5. Konfiguracja dostarczonych systemów Firewall: a. Konfiguracja podstawowych parametrów b. Konfiguracja translacji adresów NAT c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp. d. Konfiguracja inspekcji określonych protokołów sieciowych; e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall; f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; g. Testowanie działania bramy 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS: a. Konfiguracja podstawowych parametrów b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań; c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego; d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; e. Testowanie działania ochrony IPS 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. a. Przypisanie adresu IP do zarządzania. b. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3 c. Definicja reguł filtrowania/blokowania d. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny. 8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej. 9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia. 10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN.

		11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC 12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności: a. kontrola dostępu - zapora ogniowa klasy Stateful Inspection b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS] d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) f. kontrola pasma oraz ruchu [QoS, Traffic shaping] g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P h. Ochrona przed wyciekiem poufnej informacji (DLP) i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL) j. Inspekcja ruchu SSL k. Ochrony przez atakami na stacje klienckie l. Kontrola pasma 13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi. 14. Konfiguracja logowania i raportowania.
6.	**Serwer pod wirtualizację**	Zamawiający wymaga instalacji i konfiguracji dostarczonego serwera celem stworzenia bazy sprzętowej dla stworzonego systemu wirtualizacji na bazie dostarczonego serwera i oprogramowania do wirtualizacji. Serwer musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dziedzinowe.
7.	**Serwera NAS - Backup**	Urządzenie NAS należy dołączyć do infrastruktury Zamawiającego celem stworzenia miejsca na przechowywanie danych backupu.
8.	**Migracja danych**	Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów. Dane (systemy dziedzinowe) musza zostać przeniesione na nowe zasoby serwerowo-macierzowe. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych.
9.	**Serwer SMTP**	Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux.

		Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z: • Urządzeń sieciowych • Serwerów • Macierzy dyskowej • Systemu zarządzania kopiami zapasowymi • Systemu wirtualizacji serwerów • Aplikacji Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email.
10.	**Uruchomienie środowiska wirtualizacyjnego.**	Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie: 1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta. 2. Przygotowanie serwera do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 3. Przygotowanie zasobów dyskowych do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 4. Instalacja oprogramowania wirtualizacyjnego na dostarczonym serwerze. 5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów. 6. Konfiguracja i podłączenie serwera wirtualizacyjnego do zasobu dyskowego. 7. Konfiguracja i podłączenie serwera wirtualizacyjnego do sieci LAN Zamawiającego. Zamawiający wymaga, aby serwer był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 9. Przygotowanie koncepcji wirtualizacji fizycznych maszyn. 10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym. 11. Migracja istniejącej infrastruktury do środowiska wirtualnego. 12. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową 13. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
11.	**System backupu**	1. Instalacja oprogramowania zarządzającego wykonywaniem kopii zapasowych. 2. Aktywacja oraz instalacja niezbędnych licencji. 3. Konfiguracja stacji zarządzającej. 4. Dołączenie klientów do system backupu. 5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:

		a. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące; b. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy; c. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu; d. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową; e. musi istnieć możliwość odtworzenia: i. całej wirtualnej maszyny; ii. dysku wirtualnej maszyny; iii. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa); 6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej: a. Nazwę zadania backupu b. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/ c. Długość trwania zadania backupu d. Ilość zapisanych na taśmie danych 7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach: a. Błąd urządzenia b. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi c. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi d. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi e. Zdarzenia dotyczące licencji f. Zapełnienia mail-slotu 8. Uruchomienie testowych zadań backupu 9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email 10. Uruchomienie testowych zadań odtworzenia danych 11. Miejscem przechowywania kopii zapasowych jest: a. serwer NAS. b. na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym. System musi zostać podłączony do serwera wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze NAS.
12.	**Usługa katalogowa.**	**Instalacja usługi katalogowej wraz z dodatkowymi komponentami w taki sposób, aby spełnione były poniższe wymagania celem świadczenia e-usług publicznych:**
12.1.	**Zaplanowanie liczby serwerów na potrzeby**	Taka liczba serwerów, aby w przypadku awarii pojedynczego serwera był zapewniony ciągły dostęp do usługi katalogowej, a w szczególności

	usługi katalogowej oraz serwerów plików	mechanizmy uwierzytelniania oraz rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na dostarczonym środowisku wirtualizacyjnym.
12.2.	**Wersja systemu operacyjnego serwerów**	Zastosowany system operacyjny musi zapewniać, co najmniej: a) możliwość uruchomienia usługi katalogowej w trybie usługi b) możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń c) możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem (w tym przynależność do grup zabezpieczeń) d) możliwość zarządzania usługą katalogową poprzez interfejs graficzny oraz CLI e) możliwość zainstalowania lokalnego Centrum Certyfikacji zapewniającego wydawanie niekwalifikowanych certyfikatów X.509 umożliwiających uwierzytelnianie na stacjach roboczych i serwerach z wykorzystaniem kart kryptograficznych, szyfrowanie danych
12.3.	**Instalacja systemu operacyjnego serwerów**	Instalacja systemu operacyjnego serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.
12.4.	**Uruchomienie usługi katalogowej oraz niezbędnych komponentów, migracja danych do/z obecnej usługi katalogowej**	Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem. Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego. Zamawiający wymaga skonfigurowania delegacji uprawnień do zadanych jednostek organizacyjnych dla administratorów niższego poziomu. Administratorzy niższego poziomu powinni mieć uprawnienia do: a) Resetowania haseł użytkowników b) Odblokowywania kont użytkowników c) Zmiany atrybutów „Display Name” oraz „Last name” Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi: a) Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości b) Śledzenie zmian dotyczących tworzenia, usuwania obiektów

		Zamawiający wymaga skonfigurowania dwóch stacji zarządzających. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).
12.5.	**Konfiguracja polityki haseł oraz polityki blokowania kont**	Konfiguracja globalnej polityki haseł dla domeny: a) Hasło musi zawierać minimum 8 znaków b) Maksymalny czas ważności hasła: do ustalenia z Zamawiającym c) Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym d) Hasło musi spełniać zasady złożoności Konfiguracja polityki haseł dla kadry zarządzającej: a) Hasło musi zawierać minimum 10 znaków b) Maksymalny czas ważności hasła: 30 dni c) Minimalny czas, po którym możliwa jest zmiana hasła: 240 dni d) Hasło musi spełniać zasady złożoności Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach. Szczegółowe dane zostaną przekazane na etapie konfiguracji.
12.6.	**Stworzenie skryptów służących do tworzenia struktury usługi katalogowej**	Po oddaniu wdrożonego systemu do eksploatacji konieczne będzie tworzenie nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych. Zamawiający oczekuje stworzenia przez Wykonawcę skryptów ułatwiających te zadania. **Założenia skryptu tworzącego nowe jednostki organizacyjne oraz grupy:** 1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie, co najmniej: a) ścieżki i nazwy pliku wejściowego b) ścieżki i nazwy pliku logującego c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu) d) nazwy FQDN domeny e) nazwy NetBIOS domeny f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty g) ścieżek do udziałów dyskowych SHARE1 oraz SHARE2 2. Skrypt ma pobierać z pliku wejściowego listę jednostek organizacyjnych 3. Skrypt tworzy nowe jednostki organizacyjne w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu 4. Skrypt tworzy nowe grupy zabezpieczeń o nazwie G_Nazwa_Jednoski_Organizacyjnej 5. Skrypt tworzy foldery: a) \\DOMENA\Public\SHARE1 b) \\DOMENA\Public\SHARE2 Foldery muszą posiadać tak ustawione parametry zabezpieczeń, aby użytkownicy nie mogli samodzielnie tworzyć nowych katalogów ani plików w lokalizacjach \\DOMENA\SHARE1 oraz \\DOMENA\SHARE2.

		6. Skrypt tworzy podkatalogi: \\DOMENA\Public\SHARE1\Nazwa_Jednostki_Organizacyjnej oraz \\DOMENA\Public\SHARE2\Nazwa_Jednostki_Organizacyjnej 7. Skrypt nadaje uprawnienia do utworzonych podkatalogów według założeń: a) \\DOMENA\Public\SHARE1\Nazwa_Jednostki_Organizacyjnej: i. Administratorzy Domeny – Pełna kontrola ii. Grupa G_Nazwa_Jednostki_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa_Jednostki_Organizacyjnej iii. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu iv. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze a) \\DOMENA\Public\Share2\Nazwa_Jednostki_Organizacyjnej: v. Administratorzy Domeny – Pełna kontrola vi. Grupa G_Nazwa_Jednostki_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa_Jednostki_Organizacyjnej vii. Użytkownicy Uwierzytelnieni - Odczyt viii. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu ix. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 8. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 9. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania **Założenia skryptu tworzącego nowe konta użytkowników:** 1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie co najmniej: a) ścieżki i nazwy pliku wejściowego b) ścieżki i nazwy pliku logującego c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu) d) nazwy FQDN domeny e) nazwy NetBIOS domeny f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty g) ścieżki do udziału sieciowego HOME

		h) litery dysku katalogu domowego 2. Skrypt ma pobierać z pliku wejściowego listę kont użytkowników w formacie: NazwaUzytkownika;Imie;Nazwisko:Haslo;Dzial;NumerTelefonu 3. Skrypt tworzy nowe konta użytkowników w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu pobierając wszystkie niezbędne dane z pliku wejściowego 4. Nowo utworzone konta użytkowników muszą mieć jednorazowo ustawione hasła – użytkownik musi zmienić hasło podczas pierwszego logowania 5. Skrypt tworzy katalog \\DOMENA\HOME\NazwaUzytkownika 6. Skrypt nadaje uprawnienia do utworzonych katalogów użytkowników według założeń: a) Administratorzy Domeny – Pełna kontrola b) Użytkownik – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu NazwaUzytkownika c) Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu d) Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 10. Skrypt ma ustawić dla każdego konta użytkownika literę dysku domowego oraz poprawną ścieżkę sieciową 11. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 12. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania 13. Skrypt ma wygenerować dla każdego zakładanego konta osobny plik tekstowy zawierający między innymi: Nazwę użytkownika, Imię, Nazwisko, Hasło do pierwszego zalogowania. Tak utworzone pliki mogą zostać wydrukowane i przekazane użytkownikom. Powyżej opisane skrypty muszą posiadać w treści kodu stosowne komentarze opisujące działanie skryptów. Skrypty zostanę przekazane Zamawiającemu w wieczyste użytkowanie bez dodatkowych opłat wraz ze stosowną dokumentacją użytkownika oraz szczegółową instrukcja obsługi. Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów.
12.7.	**Skonfigurowanie mapowania zasobów sieciowych**	Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows. Mapowane mają być między innymi zasoby: \\DOMENA\Public\SHARE1 \\DOMENA\Public\SHARE2

		Oraz określone przez Zamawiającego drukarki sieciowe. Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby: 1. Z wykorzystaniem skryptów logowania 2. Z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows Vista i nowszych (Wymagane jest także skonfigurowanie automatycznej instalacji niezbędnych składników na stacjach klienckich. Zamawiający nie dopuszcza instalacji wymaganych składników ręcznie).
12.8.	**Uruchomienie i skonfigurowanie serwera plików oraz wydruków**	Zamawiający wymaga uruchomienie oraz skonfigurowanie serwerów plików oraz serwerów wydruków tak, aby były spełnione poniższe założenia: Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest zapewnieniem ciągłości dostępu do krytycznych danych Wnioskodawcy w przypadku awarii jednego z serwera plików. Zastosowane mechanizmy replikacji systemu plików muszą zapewniać: • Replikację multi-master z rozwiązywaniem konfliktów • Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki. Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu. Na serwerach plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów. Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących. Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwery plików. Funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego. Zamawiający wymaga stworzenie domyślnego, obowiązującego profilu wędrującego dla klienckich systemów operacyjnych. Domyślny profil ma uwzględniać opracowanie i wykonanie grafiki na pulpit komputera klienta. Grafika będzie akceptowana przez Zamawiającego. Zamawiający wymaga stworzenia i przypisania odpowiednich polityk globalnych dla wymuszenia stosowania obowiązkowych (niemodyfikowalnych) profili mobilnych. Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do

		aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji. Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi: a) Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder b) Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder c) Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień. Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera.
12.9.	**Serwery uwierzytelniające**	1. Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych. 2. Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych serwerach. 3. Instancja serwera może być uruchomiona na serwerach domenowych z zastrzeżeniem, że będzie ona kompatybilna z usługami uruchomionymi na tych serwerach i nie będzie wpływać negatywnie na ich pracę. 4. Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach. 5. Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie.
12.10.	**Dołączenie stacji roboczych do domeny**	Zamawiający wymaga dołączenia wszystkich stacji roboczych do domeny. W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mająca na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (miedzy innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na konto domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji).
12.11.	**Uruchomienie usług umożliwiającą instalację i zarządzanie aktualizacjami stacji roboczych Windows**	Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów Windows według założeń: 1. Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet 2. Administrator zatwierdza aktualizacje do instalacji

		3. Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu Zamawiający wymaga skonfigurowania co najmniej następujących parametrów: 1. Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje 2. Kategorii aktualizacji 3. Grup komputerów (KOMPUTERY, SERWERY, KOMPUTERY-TEST, SERWERY-TEST) 4. Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów 5. Zasad automatycznego zatwierdzania nowych aktualizacji. 6. Mechanizmów raportowania (email)
12.12.	**Przygotowanie infrastruktury PKI**	Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 10. Wymagana przez Zamawiającego konfiguracja zawiera co najmniej: 1. Zaplanowanie i uruchomienie wewnętrznej struktury CA 2. Konfiguracja szablonów certyfikatów 3. Wydanie certyfikatów dla serwerów oraz stacji roboczych 4. Zastosowanie mechanizmów bezpieczeństwa poprzez możliwość backupu archiwizacji kluczy prywatnych wydawanych certyfikatów. 5. Wskazanie wszystkich możliwych dróg publikacji list CRL 6. Instalacji i konfiguracji stacji (komputer PC) do wydania kart – stacja do personalizacji.
13.	**Testowanie i modyfikacja parametrów infrastruktury sieciowej.**	1. Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego. 2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. 3. Testowanie mechanizmów replikacji danych. 4. Testowanie dostępu publicznego do zasobów. 5. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu 6. Testowanie autoryzowanego dostępu do wewnętrznych zasobów. 7. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach
14.	**Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.**	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą. **Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.** W tym czasie przedstawiciel Wykonawcy: • zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji.

		• dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności: a) zastosowanej technologii serwerów b) zastosowanej technologii pamięci masowej c) wirtualizacji d) systemu backupu e) zastosowanych rozwiązań aplikacyjnych f) sieci LAN g) systemu firewall Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania.
15.	**Opracowanie dokumentacji powykonawczej**	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu. 1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów. 2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację). 3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały. 5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.

5.9. Diagnoza cyberbezpieczeństwa

Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina", opisanymi na stronie https://www.gov.pl/web/cppc/cyfrowa-gmina

Wykonawca musi wykonać usługę zgodnie zakresem oraz z formularzem stanowiącym załącznik do dokumentacji konkursowej. załączniku nr
Załącznik_nr_8_-_Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa

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.