Opis przedmiotu zamówienia

Część 1

- 22 zestawy komputerowe dla Urzędu (komputer, mysz, klawiatura, system operacyjny Windows 11 Pro + monitor)
- 9 zestawów komputerowych dla OPS (komputer, mysz, klawiatura, system operacyjny Windows 11 Pro + monitor)
- 16 stacji roboczych dla Urzędu (komputer, mysz, klawiatura, system op. Windows 11 Pro)
- 5 stacji roboczych dla OPS (komputer, mysz, klawiatura, system op. Windows 11 Pro)
- 3 monitory LCD dla Urzędu
- 4 laptopy 15,6” dla Urzędu
- 2 laptopy 14” dla Urzędu

Łącznie: 52 jednostki komputerowe (stacje robocze), 34 monitory, 6 laptopów (w tym 4 x 15,6-calowe oraz 2 x 14-calowe)

Specyfikacja dla pojedynczej jednostki komputerowej:

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Komputer - Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna		
1.	Obudowa	Typu small form factor z obsługą kart PCI Express wyłącznie o niskim profilu. Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. na napęd optyczny (dopuszcza się stosowanie napędów slim) zewnętrzna, 1 szt. 3,5”na standardowy dysk twardy. Wyposażona w czytnik kart multimedialnych - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym - Wyposażona w budowany głośnik o mocy min. 1.5W
2.	Zasilacz	Zasilacz maksymalnie 260W o sprawności minimum 85%
3.	Chipset	Dostosowany do zaoferowanego procesora
4.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera. Wyposażona w złącza min.: - 1 x PCI Express 3.0 x16, - 1 x PCI Express 3.0 x1, - 2 x M.2 z czego min. 1 przeznaczona dla dysku SSD z obsługą PCIe NVMe
5.	Procesor	Minimum 12 320 punktów na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/
6.	Pamięć operacyjna	Min. 8GB DDR4 2666MHz z możliwością rozszerzenia do 32 GB Ilość banków pamięci: min. 2 szt. Ilość wolnych banków pamięci: min. 1 szt.
7.	Dysk twardy	Min 512GB SSD M.2 PCIe NVMe zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na

		komputerze po awarii.
8.	Napęd optyczny	Nagrywarka DVD +/-RW
9.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.
10.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.
11.	Karta sieciowa	LAN 10/100/1000 Mbit/s z funkcją PXE oraz Wake on LAN
12.	Porty/złącza	Wbudowane porty/złącza: Wideo różnego typu umożliwiające elastyczne podłączenie urządzenia bez stosowania przejściówek lub adapterów za pomocą min: - 1 x VGA, - 1 x HDMI Pozostałe porty/złącza: - 8 x USB w tym: - z przodu obudowy min. 4 x USB3.2 - z tyłu obudowy min. 4 x USB z czego min. 2x USB3.2 - port sieciowy RJ-45, - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy - port szeregowy - czytnik kart pamięci 7-in-1 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
13.	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera, PN - numerze seryjnym, - AssetTag, - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku i napędu optycznego) Możliwość z poziomu Bios: - wyłączania/włączania portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych

		z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów - alertowania zmiany konfiguracji sprzętowej komputera - załadowania optymalnych ustawień Bios - obsługa Bios za pomocą klawiatury i myszy
14.	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego lub SSD • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej • test myszy i klawiatury • test procesora Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja oraz data wydania Bios • Procesor: Nazwa, taktowanie • Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk: model, numer seryjny, wersja firmware, pojemność, temperatura pracy • Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
15.	Certyfikaty i standardy	- Certyfikat ISO9001 lub równoważny przedmiotowy środek dowodowy dla producenta sprzętu, dotyczący zarządzania jakością, zgodnie z treścią art. 105 ust. 3 i 4 pzp (należy załączyć do oferty) - Deklaracja zgodności CE (załączyć do oferty) - Głośność jednostki mierzona z pozycji operatora w trybie IDLE nie większa niż 22 dB – (załączyć do oferty dokument potwierdzający głośność jednostki)

		- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych – oświadczenie wykonawcy złożone podczas dostawy
16.	Waga/rozmiary urządzenia	Waga urządzenia poniżej 5 kg Wysokość nie może być większa niż 32cm Szerokość nie może być większa niż 10cm
17.	Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock - Oczko na kłódkę
18.	Gwarancja	3 lata świadczona w miejscu użytkowania sprzętu (on-site)
19.	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. - możliwość weryfikacji u producenta konfiguracji fabrycznej zakupionego sprzętu - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.

Klawiatura - klawiatura przewodowa w układzie US

Mysz - mysz przewodowa (scroll)

System operacyjny

System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego
3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
9. Wbudowany system pomocy w języku polskim.
10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.

13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
24. Wbudowany mechanizm wirtualizacji typu hypervisor."
25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
34. Możliwość tworzenia wirtualnych kart inteligentnych.
35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.

37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
38. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty inteligentne i certyfikaty (smartcard),
    c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
    d. Certyfikat/Klucz i PIN
    e. Certyfikat/Klucz i uwierzytelnienie biometryczne
39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5
40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.
41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń
43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń

Monitor - będzie wykorzystywany dla potrzeb aplikacji biurowych, obróbki zdjęć lub wideo

Monitor musi być fabrycznie nowy

Przekątna ekranu: min. 23,8”, format obrazu 16:9

Matryca typu IPS/PLS/MVA/WVA o wykończeniu matowym (nie dopuszcza się naklejek matowiących matrycę)

Czas reakcji max. 4ms

Nominalna rozdzielczość i wielkość piksela: rozdzielczość nie mniejsza niż FHD (1920x1080), piksel nie większy niż 0.28 mm

Kąty widzenia min. 178 stopni w pionie i min. 178 stopni w poziomie

Zakres kolorów nie mniejszy niż 72% NTSC, Kontrast nie mniejszy niż: 1000:1, Jasność nie mniejsza niż 250 cd/m2

Minimalna ilość dostępnych złącz monitora: 1x HDMI, 1x VGA

Do monitora należy dołączyć minimum kable HDMI, VGA, Kabel zasilający

Stopa lub podstawa monitora musi umożliwiać: przechylenie w pionie min. 25 stopni (-5 / 20), regulację wysokości min. 15 cm

Obudowa powinna posiadać wbudowane w obudowę przyciski umożliwiające włączenie, wyłączenie oraz zmianę ustawień wyświetlania monitora, powinna być trwale oznaczona nazwą producenta, numerem seryjnym i katalogowym pozwalającym na jednoznaczną identyfikację zaoferowanego monitora, jeżeli zasilacz monitora nie jest wbudowany w obudowie, należy dostarczyć oryginalny zasilacz zewnętrzny wyprodukowany przez producenta monitora

Wymagane certyfikaty: - Energy Star 8.0 - Deklaracja zgodności CE (załączyć do oferty) - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych – oświadczenie wykonawcy złożone podczas dostawy Gwarancja min. 36 miesięcy Wsparcie techniczne powinno obejmować dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej, możliwość weryfikacji na stronie producenta posiadanej gwarancji, możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego

Specyfikacja pojedynczego komputera przenośnego - laptopa 15,6 calowego (4 sztuki):

Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający.		
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne**
20.	Procesor	Minimum 10 090 punktów na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/
21.	Pamięć operacyjna RAM	Min. 8 GB 3200 MHz non-ECC Możliwość rozbudowy pamięci do min. 40GB
22.	Parametry pamięci masowej	M.2 256 GB SSD PCIe NVMe Dostępny drugi slot M.2 na dysk SSD. Możliwość rozbudowy do konfiguracji dwudyskowej.
23.	Karta graficzna	Zintegrowana z procesorem
24.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby Audio stereo (2x2W), port słuchawek i mikrofonu typu COMBO, kamera video 720p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).
25.	Obudowa	Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H lub równoważne.
26.	Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej.

27.	Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym
28.	Bezpieczeństwo	TPM 2.0 Slot umożliwiający fizyczne zabezpieczenie komputera np. Kensington
29.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
30.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM - typie procesora i jego prędkości - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość ustawienia hasła Administratora - Możliwość ustawienia hasła Użytkownika - Możliwość ustawienia hasła dysku twardego - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS - Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth
31.	Ekran	Matowy, matryca TFT 15” z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, 300nits, kontrast 800:1 w technologii IPS/PLS/WVA Kąt otwarcia pokrywy ekranu min.180 stopni.
32.	Interfejsy / Komunikacja	4xUSB 3.2 z czego minimum 2 złącza Typu-C umożliwiające podłączenie stacji dokującej lub zasilania notebooka i dodatkowego ekranu (niezależnie od wybranego portu USB-C). Złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. 1.4b, RJ-45. Komputer musi obsługiwać komunikację

		Thunderbolt 4 za pomocą min. 1 złącza USB-C. Czytnik kart pamięci.
33.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX 2x2 Bluetooth 5.1
34.	Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w 2 stopniowe podświetlanie przycisków.
35.	Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych w przycisku zasilania
36.	Akumulator	Pozwalający na nieprzerwaną pracę urządzenia do min. 6 godzin – załączyć kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 30 minut od 0% do 50%.
37.	Zasilacz	Zasilacz zewnętrzny 65W
38.	Certyfikaty, oświadczenia i standardy	- Produkt spełniający normy: o ISO 9001 o ISO 14001 o ISO 50001 - Komputer spełniający: o Mil-STD-810H o Ochronę oczu TÜV Low Blue Light o Deklaracja zgodności CE o Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych – oświadczenie wykonawcy złożone podczas dostawy o Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy (IDLE) wynosząca maksymalnie 20 dB
39.	Waga/Wymiary	Waga urządzenia z akumulatorem do 1,85 kg Grubość notebooka nie większa niż: 19 mm
40.	System operacyjny	Microsoft Windows 10 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia

		aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.

		20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia

		zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
41.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
42.	Gwarancja	Minimalny czas trwania gwarancji producenta wynosi 3 lata, świadczona w miejscu użytkowania sprzętu (on-site). Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń - Zamawiający zastrzega sobie prawo do możliwości weryfikacji powyższego wymogu. W przypadku weryfikacji przez Zamawiającego, Wykonawca dostarczy stosowne dokumenty.
43.	Wsparcie techniczne producenta	▪ Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera ▪ Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. ▪ Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera ▪ Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online,

		dostępna w dni powszednie od 9:00-18:00 Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.

Specyfikacja pojedynczego komputera przenośnego - laptopa 14 calowego:

Szczegółowy opis		
Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający.		
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne**
44.	Procesor	Minimum 6 650 punktów na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/
45.	Pamięć operacyjna RAM	Min. 8 GB non-ECC Możliwość rozbudowy pamięci do min. 32GB
46.	Parametry pamięci masowej	M.2 256 GB SSD PCIe NVMe Dostępny drugi slot M.2 na dysk SSD. Możliwość rozbudowy do konfiguracji dwudyskowej.
47.	Karta graficzna	Zintegrowana z procesorem
48.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby Audio stereo (2x2W), port słuchawek i mikrofonu typu COMBO, kamera video 720p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).
49.	Obudowa	Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H.
50.	Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej.
51.	Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym.
52.	Bezpieczeństwo	TPM 2.0 Slot umożliwiający fizyczne zabezpieczenie komputera np. Kensington
53.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu

		(możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
54.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM - typie procesora i jego prędkości - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość ustawienia hasła Administratora - Możliwość ustawienia hasła Użytkownika - Możliwość ustawienia hasła dysku twardego - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS - Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth
55.	Ekran	Matowy, matryca TFT 14” z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, 250nits, kontrast 800:1 w technologii IPS/PLS/WVA Kąt otwarcia pokrywy ekranu min.180 stopni.
56.	Interfejsy / Komunikacja	2xUSB 3.0. Złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. 1.4b, RJ-45. Czytnik kart pamięci.
57.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX 2x2 Bluetooth
58.	Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w 2 stopniowe podświetlanie przycisków.
59.	Akumulator	Pozwalający na nieprzerwaną pracę urządzenia do min. 6 godzin – załączyć kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 30 minut od 0% do 50%.

60.	Zasilacz	Zasilacz zewnętrzny 65W
61.	Certyfikaty, oświadczenia i standardy	- Produkt spełniający normy: o ISO 9001 o ISO 14001 o ISO 50001 - Komputer spełniający: o Mil-STD-810H o Ochronę oczu TÜV Low Blue Light o Deklaracja zgodności CE o Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych – oświadczenie wykonawcy złożone podczas dostawy o Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy (IDLE) wynosząca maksymalnie 20 dB (załączyć kartę katalogową)
62.	Waga/Wymiary	Waga urządzenia z akumulatorem do 1,85 kg Grubość notebooka nie większa niż: 19 mm
63.	System operacyjny	Microsoft Windows 10 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.

		8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 24. Wbudowany mechanizm wirtualizacji typu hypervisor. 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa

		związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera

		poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
64.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
65.	Gwarancja	Minimalny czas trwania gwarancji producenta wynosi 3 lata, świadczona w miejscu użytkowania sprzętu (on-site). Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń - Zamawiający zastrzega sobie prawo do możliwości weryfikacji powyższego wymogu. W przypadku weryfikacji przez Zamawiającego, Wykonawca dostarczy stosowne dokumenty.
66.	Wsparcie techniczne producenta	▪ Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera ▪ Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. ▪ Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera ▪ Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00 Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.

Część 2

78 zasilaczy awaryjnych UPS:

- 63 zasilacze awaryjne UPS dla Urzędu
- 15 zasilaczy awaryjnych UPS dla OPS-u

Specyfikacja pojedynczego zasilacza UPS:

1.	UPS 550VA (parametry minimalne)	Urządzenie musi być fabrycznie nowe. Parametr/Wymagania minimalne moc pozorna: min. 550VA moc rzeczywista: min. 330W Technologia: VI (line interactive) Typ obudowy: wolnostojąca
2.	praca sieciowa	Napięcie wejściowe: 162 ÷ 290 V AC ± 7 V Częstotliwość napięcia wejściowego: 40 ÷ 70 Hz ± 1 Hz Zakres napięcia wyjściowego: 230 V AC ± 10 % Kształt napięcia wyjściowego: Schodkowa aproksymacja sinusoidy / Tak jak na wejściu Progi przełączania sieć – UPS: 162 ÷ 290 V AC ± 7 V Czas przełączania sieć – UPS: <6ms
3.	praca bateryjna	Napięcie wyjściowe: ~230V ± 10% Częstotliwość napięcia wyjściowego: 50 / 60 Hz ± 1% Kształt napięcia wyjściowego na pracy bateryjnej: Schodkowa aproksymacja sinusoidy Progi przełączania UPS – sieć: ~172 ÷ 280 V ± 7 V Przeciążalność: > 110% - 1 min (wyłączenie UPS – praca sieciowa i bateryjna) Zabezpieczenie wyjściowe przeciwzwarciowe: elektroniczne Zabezpieczenie wyjściowe przeciążeniowe: elektroniczne Czas podtrzymania (P 0,8max/P 0,5max): minimum 2/6 min akumulatory wewnętrzne: minimum 12V5Ah; szczelne, bezobsługowe VRLA
4.	pozostałe	Ilość i typ gniazd wyjściowych: minimum 2 gniazda z podtrzymaniem standardu PL (z bolcem uziemiającym) + minimum 1 gniazdo z podtrzymaniem standardu IEC 320 C13 (10 A) Zimny Start: tak Interfejs komunikacyjny: USB HID (kabel w komplecie) Automatyczna regulacja napięcia AVR: wymagana Waga UPS: do 4kg Wymiary: nie większe niż: wysokość 160 mm; szerokość 85 mm; głębokość 255 mm gwarancja: min 24 miesiące na elektronikę i 12 miesięcy na akumulatory; serwis: autoryzowany serwis producenta zlokalizowany w Polsce, serwis realizowany w systemie door-to-door
5.	sygnalizacja	Akustyczno-optyczna Dioda sygnalizująca minimum pracę sieciową, bateryjną, niski poziom baterii, przeciążenie, awarię Sygnalizacja akustyczna informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu, awarii
6.	oprogramowanie	- oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS.

		- wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. - możliwość edycji nazw urządzeń na liście monitorowanych UPS-ów - wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer
7.	certyfikaty producenta (załączyć do oferty)	ISO 9001:2015 lub równoważnego dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - deklaracja CE

Część 3

105 licencji oprogramowania- Oprogramowanie Microsoft Office Home & Business 2021 BOX lub równoważnego

- 80 licencji dla Urzędu
- 25 licencji dla OPS-u

<u>Specyfikacja pojedynczego pakietu</u>:

Pakiet aplikacji biurowych oczekiwany przez Zamawiającego: Microsoft Office Home and Business 2021 PL. Zamawiający dopuszcza zaproponowanie oprogramowania równoważnego - za oprogramowanie równoważne Zamawiający uznaje Oprogramowanie posiadające tożsamą funkcjonalność co wskazane w opisie przedmiotu zamówienia		
1.	Wymagania minimalne	Pakiet biurowy dostarczony wraz z licencją na czas nieokreślony z nośnikiem lub w wersji umożliwiającej pobranie oprogramowania ze strony producenta. Rok produkcji pakietu aplikacji biurowych - po roku 2020
2.	Wymagania odnośnie interfejsu użytkownika	Pełna polska wersja językowa interfejsu użytkownika. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nie posiadającym umiejętności technicznych. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
3.	Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki	- posiada kompletny i publicznie dostępny opis formatu, - ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2005.212.1766), - umożliwia wykorzystanie schematów XML, wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych

		(Dz.U.2005.212.1766) Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy), Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. Pakiet zintegrowanych aplikacji biurowych musi zawierać: 1)Edytor tekstów 2)Arkusz kalkulacyjny 3)Narzędzie do przygotowywania i prowadzenia prezentacji 4)Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) Edytor tekstów musi umożliwiać: • Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. • Wstawianie oraz formatowanie tabel i obiektów graficznych. • Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). • Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel, rysunków oraz tworzenie spisów treści. • Formatowanie nagłówków i stopek stron. • Sprawdzanie pisowni w języku polskim. • Śledzenie zmian wprowadzonych przez użytkowników. • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. • Określenie układu strony (pionowa/pozioma). • Wydruk dokumentów. • Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. • Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010, 2013, 2016, 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów Dokumentu. • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. • Wymagana jest dostępność do oferowanego edytora

		tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem. • Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. • Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych. Arkusz kalkulacyjny musi umożliwiać: • Tworzenie raportów tabelarycznych i wykresów liniowych (wraz linią trendu), słupkowych, kołowych. • Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. • Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). • Obsługę „kostek OLAP” oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. • Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. • Wyszukiwanie i zamianę danych. • Wykonywanie analiz danych przy użyciu formatowania warunkowego. • Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. • Formatowanie czasu, daty i wartości finansowych z polskim formatem. • Zapis wielu arkuszy kalkulacyjnych w jednym pliku. • Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010, 2013, 2016 I 2019 z uwzględnieniem

		poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: • Przygotowywanie prezentacji multimedialnych, które będą: ▪ Prezentowane przy użyciu projektora multimedialnego. ▪ Drukowane w formacie umożliwiającym robienie notatek. ▪ Zapisane jako prezentacja tylko do odczytu. • Nagrywanie narracji i dołączanie jej do prezentacji. • Opatrywanie slajdów notatkami dla prezentera. • Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. • Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. • Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. • Możliwość tworzenia animacji obiektów i całych slajdów. • Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. • Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007 2010, 2013, 2016 i 2019. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: • Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. • Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. • Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. • Automatyczne grupowanie poczty o tym samym tytule. • Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. • Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia. • Zarządzanie kalendarzem. • Udostępnianie kalendarza innym użytkownikom. • Przeglądanie kalendarza innych użytkowników. • Zapraszanie uczestników na spotkanie, co po ich akceptacji

		powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. • Zarządzanie listą zadań. • Zlecanie zadań innym użytkownikom. • Zarządzanie listą kontaktów. • Udostępnianie listy kontaktów innym użytkownikom. • Przeglądanie listy kontaktów innych użytkowników. • Możliwość przesyłania kontaktów innym użytkowników.

Wykonawca zobowiązany jest dołączyć do oferty następujące dokumenty:
- opis proponowanego rozwiązania potwierdzający, że oferowany Pakiet aplikacji biurowych spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta oraz wersji oferowanego Pakietu aplikacji biurowych

Część 4

Jedna licencja systemu operacyjnego Windows Server 2019 Standard lub równoważna dla OPS

<u>Specyfikacja oprogramowania:</u>

Licencja Windows Server 2019 Standard 64bit EN lub rozwiązanie równoważne

1 sztuka licencji Windows Server 2019 Standard 64bit EN lub równoważnej zgodnie z opisem poniżej.

Licencja wieczysta.

Oprogramowanie równoważne dla wymienionego powyżej oprogramowania:

Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Współpraca z procesorami o architekturze x86-64.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. W ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wyposażonym w 2 rdzenie.
4. Praca w roli serwera domeny Microsoft Active Directory.
5. Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).
6. Zawarta możliwość uruchomienia roli serwera DNS.
7. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP).
8. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.

9. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Zawarta możliwość uruchomienia roli serwera stron WWW.
11. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
12. W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego, minimalnie przez okres 4 lat bez dodatkowych kosztów, licząc od dnia zawarcia umowy dostawy.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Oprogramowanie wydane po 2017 roku.

Część 5

Trzy zarządzalne przełączniki sieciowe 48-portowe o przepustowości min. 1 Gb/s z usługą wymiany urządzenia w razie awarii (dla Urzędu):

<u>Specyfikacja pojedynczego urządzenia:</u>

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:		
1	**Parametry fizyczne platformy**	Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V. Maksymalny pobór mocy: 60 W. Minimalny zakres temperatury pracy: 0-40°C
2	**Interfejsy sieciowe - wymagania minimalne**	Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: - 48 porty GE RJ-45. - 4 porty 10 GE SFP+.
3	**Zarządzanie**	• Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz

		zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
4	**Parametry wydajnościowe**	• Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. • Tablica adresów MAC o pojemności co najmniej 32k wpisów. • Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
5	**Wymagane funkcje**	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
6	**Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC**	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania

		• Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
7	**Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa**	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
8	**Gwarancja oraz wsparcie**	System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, 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.
9	**Rozszerzone wsparcie serwisowe**	1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy. 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie

		świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7

Część 6

Zapora sieciowa UTM wraz ze wsparciem (dla Urzędu)

<u>Specyfikacja urządzenia:</u>

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:

- Firewall.
- Ochrony w warstwie aplikacji.
- 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.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 5 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 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 5 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 64 B.
4. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 1518 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
6. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
7. 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 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 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
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - Nuage Networks VSP.
   - OpenStack.
   - VMware vCenter (ESXi).
   - VMware NSX.

· VMware NSX.Nutanix
· VMware NSX.IBM Cloud

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.
3. Rozwiązanie powinno wspierać funkcję Forward Error Correctionm na tunelach IPSec.
4. Funkcja monitorowania łącza w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.

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. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
9. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla servisów youtube, vimeo.
10. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.

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 lub równoważne.

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 na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, 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.

Rozszerzone wsparcie serwisowe AHB/SOS

a) System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.

- Wraz z dostawą wykonawca poda adres strony internetowej serwisu i numer infolinii telefonicznej.
- Certyfikat ISO 9001 podmiotu serwisującego.

Część 7

Oprogramowanie do szyfrowania dysków oraz nośników pamięci zewnętrznej 100 licencji 4-letnich dla Urzędu

<u>Specyfikacja oprogramowania:</u>

100 licencji oprogramowania do szyfrowania komputerów wraz ze wsparciem technicznym i prawem do aktualizacji na 4 lata:

1. Oprogramowanie musi zapewnić możliwość centralnego zarządzania systemem szyfrowania i jego konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność:
    1.1. wyświetlać komputery wraz z dyskami systemowymi oraz dyskami podłączonymi do komputera
    1.2. umożliwiać włączenie szyfrowania na wybranych dyskach
    1.3. możliwość szyfrowania dysków systemowych
    1.4. szyfrowanie/deszyfrowanie dysków w trakcie pracy użytkownika na komputerze
    1.5. wyświetlać zbiorcze raporty, które komputery są szyfrowane, a które nie
    1.6. wyświetlać zdarzenia jakie są wykonywane podczas szyfrowania:
        1.6.1. postęp szyfrowania/deszyfrowania
        1.6.2. logi z wykonywanych operacji zapisane w centralnej bazie
    1.7. wyświetlać listę dysków jakie były podłączane do komputerów
2. Oprogramowanie instalowane na komputerze musi zapewnić funkcjonalność:
    2.1. umożliwiać zdalną instalację agentów na wybranych komputerach
    2.2. umożliwiać instalację oprogramowania w trybie cichym bez ingerencji użytkownika
    2.3. wsparcie dla dysków HDD i SSD
    2.4. możliwość szyfrowania dysków lokalnych i wymiennych FAT32, NTFS algorytmem AES
    2.5. wsparcie dla systemu Windows: 7, 8, 8.1, 10,11 w wersji pro i home
    2.6. system musi informować użytkownika o postępie szyfrowania dysku
    2.7. system musi wznawiać szyfrowanie dysku w przypadku resetu, wyłączenia lub zawieszenia komputera
    2.8. system musi poinformować użytkownika o procesie szyfrowania w momencie gdy użytkownik będzie chciał go poprawnie wyłączyć lub zrestartować. Aplikacja powinna oprócz takiego poinformowania dać możliwość wyboru użytkownikowi czy system sam automatycznie ma się wyłączyć po zakończeniu szyfrowania, czy też nie
3. Licencja oprogramowania musi być licencją bezterminową na użytkowanie z dwuletnim wsparciem technicznym i prawem do aktualizacji.

Część 8

Oprogramowanie dla Urzędu zabezpieczającego wewnętrzną i zewnętrzną korespondencję e-mail, 130 sztuk w tym:
100 licencji 4-letnich dla Urzędu
30 licencji 4-letnich dla OPS-u

Specyfikacja oprogramowania:

100 (Urząd) / 30 (OPS) Licencji oprogramowania do szyfrowania wiadomości email technologią END TO END. Wsparcie techniczne i prawo do aktualizacji na 4 lata. Bazy reguł, sygnatur i zagrożeń phishing na 4 lata.

1. Oprogramowanie musi zapewnić funkcjonalność:
    1.1. szyfrowanie algorytmem AES256 treści wiadomości,
    1.2. szyfrowanie algorytmem AES256 załączników,
    1.3. szyfrowanie algorytmem AES256 plików,
    1.4. szyfrowanie algorytmem AES256 katalogów,
    1.5. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagana jest dodatkowa płatna lub bezpłatna licencja (oprogramowanie, usługa, chmura, hosting) lub dostęp do portalu internetowego.
    1.6. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe.
    1.7. odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11,Ubuntu Desktop 20.04.3 ,Ubuntu Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0
    1.8. generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania,
    1.9. opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność,
    1.10. zabezpieczenia każdego emaila dedykowanym unikalnym hasłem,
    1.11. posiadania wewnętrznej bazy haseł, która umożliwia:
        1.11.1. export haseł do pliku,
        1.11.2. import haseł z pliku
        1.11.3. generowania ponownie haseł w bazie
    1.12. posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich,
    1.13. posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym,
    1.14. posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych, plików i katalogów,
    1.15. umożliwienia pracy i pomocy zdalnej użytkownikom poprzez przejęcie zdalnego pulpitu również poza siecią lokalną z użyciem jednorazowych wygenerowanych kodów autoryzacyjnych. Dodatkowo system pracy zdalnej musi działać niezależnie od włączonej funkcji UAC w systemie Windows.
    1.16. integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym,
    1.17. zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe,
    1.18. wykrywania fałszywych emaili - Antiphishing,
    1.19. wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,

1.20. wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych,
1.21. wykrywanie niebezpiecznych dokumentów MS Office,
1.22. wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,
1.23. definiowania alarmów informujących o niebezpiecznych mailach i załącznikach,
1.24. współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 2 lata.
1.25. współpracy z klientem Mozilla Thunderbird i Mozilla Thunderbird Portable dla systemów 32 i 64 Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11.

2. Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy.

3. Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy.

4. Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami.

5. Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.

6. Oprogramowanie musi zawierać moduł szkoleniowy, umożliwiający przeprowadzanie cyklicznych zdalnych szkoleń minimum raz w roku z tematyki cyberbezpieczeństwa, zagrożeń poczty e-mail, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001 lub uprawnienia równoważne przez 4 lata.

Część 9

Rozwiązanie serwerowe z funkcjonalnością kontrolera domeny, wirtualizacji, backupu, monitorowania komputerów, szyfrowania dysków, skanera podatności i luk w oprogramowaniu użytkowym wraz z serwerem zapasowym dla zapewnienia ciągłości działania (dla OPS-u)

<u>Specyfikacja rozwiązania:</u>

W ramach postępowania wymaganym jest dostarczenie rozwiązania serwerowego z funkcjonalnością kontrolera domeny, wirtualizacji, backupu, monitorowania komputerów, szyfrowania dysków, skanera podatności i luk w oprogramowaniu użytkowym, na które składają się serwer główny i zapasowy, odpowiednie oprogramowanie oraz usługa wdrożenia rozwiązania:

Serwer główny:
1. Obudowa: RACK 1U
2. Procesor: Jeden procesor czterordzeniowy z obsługą instrukcji 64-bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na

stronie http://www.cpubenchmark.net/high_end_cpus.html. Procesor z obsługą wirtualizacji.
3. Pamięć: min. 32GB dedykowane do pracy serwerowej
4. 4 kieszenie HotSwap SATA3
5. 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap
6. 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap.
7. Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s
8. Wsparcie KVM przez LAN
9. Panel przedni chroniący kluczem dostępu do dysków
10. Czujnik otwarcia obudowy
11. Komplet szyn montażowych w zestawie
12. Gwarancja: 2 lata gwarancji producenta.

Serwer zapasowy:
1. Obudowa: RACK 1U
2. Procesor: Jeden procesor czterordzeniowy z obsługą instrukcji 64-bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie http://www.cpubenchmark.net/high_end_cpus.html. Procesor z obsługą wirtualizacji.
3. Pamięć: min. 32GB dedykowane do pracy serwerowej
4. 4 kieszenie HotSwap SATA3
5. 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap
6. 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap.
7. Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s
8. Wsparcie KVM przez LAN
9. Panel przedni chroniący kluczem dostępu do dysków
10. Czujnik otwarcia obudowy
11. Komplet szyn montażowych w zestawie
12. Gwarancja: 2 lata gwarancji producenta.

Oprogramowanie serwera zarządzania komputerami przy pomocy kontrolera domeny, oprogramowanie do szyfrowanie dysków twardych i pamięci zewnętrznych, wsparcie techniczne i prawo do aktualizacji na 2 lata:

1. Oprogramowanie dostarczone razem z serwerami musi zapewnić możliwość zarządzania systemem i konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność:
    1.1. interfejs obsługi serwera musi być realizowany przez najnowsze przeglądarki internetowe i być w standardzie Windows METRO,
    1.2. system powinien przed zalogowaniem do panelu zarządzającego informować w czasie rzeczywistym administratora o obciążeniu: całego systemu, procesora, pamięci oraz interfejsu sieciowego na dynamicznych wykresach. Wskazując myszką dane na wykresie powinny pokazywać wartość obciążenia. Informacje o obciążeniu całego systemu, procesora, pamięci oraz interfejsu sieciowego powinny być archiwizowane w serwerze i dostępne przez system raportujący dla okresów: godzinowy, dzienny, tygodniowy i miesięczny,
    1.3. serwer musi umożliwiać realizowanie usług (FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS),

1.4. musi posiadać zainstalowane oprogramowanie antywirusowe,
1.5. możliwość zarządzania serwerem poprzez protokół SNMP w wersji 1/2/3,
1.6. musi umożliwiać dostęp administratorów przez przeglądarkę WEB,
1.7. musi posiadać wbudowany firewall dostępny przez przeglądarkę WEB,
1.8. przed zalogowaniem administratora do interfejsu serwera WEB, powinien bez autoryzacji odczytywać parametry obciążenia serwera pokazywane na dynamicznych wykresach w przeglądarce WEB,
1.9. system musi umożliwiać generowanie certyfikatów SSL przez przeglądarkę WEB,
1.10. system powinien posiadać możliwość importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB,
2. W zakresie obsługi domeny, dostarczone oprogramowanie musi zapewnić funkcjonalność:
2.1. zarządzania do min. 30 użytkowników, grup,
2.2. zarządzanie do min. 30 komputerów,
2.3. zarządzanie do min. 30 urządzeń,
2.4. zarządzania polisami GPO,
2.5. obsługę profili użytkowników oraz profili mobilnych,
2.6. obsługę do min. 50 jednoczesnych podłączeń do serwera domeny,
2.7. zarządzania użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego przez przeglądarkę WEB,
2.8. możliwość tworzenia użytkowników i grup w kontrolerze domeny przez przeglądarkę WEB,
2.9. nadawania haseł dla użytkowników w kontrolerze domeny przez przeglądarkę WEB,
2.10. wyszukiwania po nazwie użytkownika, grupy i komputera przez przeglądarkę WEB,
2.11. listy użytkowników, którym wygasła ważność konta dostępna w przeglądarce WEB,
2.12. listy zablokowanych kont w kontrolerze domeny dostępna w przeglądarce WEB,
2.13. wszystkie operacje zakładania i modyfikacji oraz usuwania kont, grup, komputerów w kontrolerze domenowym przez przeglądarkę WEB powinny być raportowane w centralnym repozytorium systemowym,
2.14. możliwość wyświetlenia oraz akceptowania polityki bezpieczeństwa przed zalogowaniem użytkowników do serwera domenowego,
2.15. administrator podłączający się do kontrolera domeny musi mieć możliwość autoryzacji i logowania się do serwera domenowego przy pomocy jednego dostarczonego do serwera urządzenia sprzętowego token wykorzystującego port USB,
2.16. administrator zanim dokona logowania do kontrolera domeny przy pomocy urządzenia sprzętowego token może wyświetlić wewnętrzną politykę bezpieczeństwa informacji Jednostki Organizacyjnej. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny.
2.17. administrator wyciągając urządzenie autoryzacyjne token z portu USB będzie miał blokowany system operacyjny.
2.18. zastosowane urządzenie sprzętowe token powinno umożliwiać przypisywanie konkretnego komputera (wraz z logowaniem administratora do kontrolera domeny) do urządzenia sprzętowego token,

2.19. pamięć urządzenia sprzętowego token musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domeny,

2.20. urządzenie sprzętowe token musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0,

2.21. urządzenie sprzętowe token w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u,

2.22. współpraca z klientami Windows 7, 8, 8.1, 10, 11 w wersji Professional.

3. Licencja kontrolera domeny dla zamawianego serwera głównego i zapasowego musi umożliwiać:

3.1. łatwe przenoszenie i uruchomienie kontrolera domeny pomiędzy zamawianym serwerem głównym i zapasowym,

3.2. łatwe uruchomienie kontrolera domeny w trybie awaryjnym (w ograniczonej funkcjonalności) na dowolnym serwerze posiadanym przez zamawiającego na czas naprawy zamówionego serwera głównego lub zapasowego.

4. Oprogramowanie musi umożliwiać wirtualizację dowolnych systemów operacyjnych i musi realizować:

4.1. obsługę minimum cztero-rdzeniowego procesora,

4.2. obsługę minimum 32GB RAM-u,

4.3. obsługę vmware VMDK,

4.4. obsługę minimum 10 instancji środowisk wirtualnych,

4.5. zapis stanu maszyny wirtualnej tzw. snapshot,

4.6. kopii stanu maszyny wirtualnej,

4.7. emulacji wielu urządzeń np. kart sieciowych, kontrolerów SAS,

4.8. dynamicznej alokacji pamięci na kontener danych

4.9. współpracy z kontrolerami SATA, SCSI,

4.10. tryb pracy sieciowej min NAT, tunel UD, Bridge oraz wielu interfejsów sieci,

4.11. zarządzanie poprzez przeglądarkę WEB,

4.12. archiwizacje uruchomionych maszyn wirtualnych.

5. Wykonawca musi dostarczyć oprogramowanie umożliwiające migrację użytkowników lokalnych do serwera domenowego działającego w systemie Windows Vista, 7, 8, 8.1, 10, 11 w wersji 32 i 64 bity w wersji Professional z licencją na użytkowanie bezterminową umożliwiając przenoszenie do 50 użytkowników i musi realizować:

5.1. automatyczne przenoszenie profili i ustawień użytkownika z konta lokalnego do konta domenowego,

5.2. automatyczne przeniesienie dokumentów użytkownika z konta lokalnego do konta domenowego i nadanie odpowiednich uprawnień ACL,

5.3. automatyczne przenoszenie uprawnień plikowych i rejestru z konta lokalnego do konta domenowego

5.4. automatyczne przeniesienie lokalnej skrzynki pocztowej Microsoft Outlook i Thunderbird z domyślnej lokalizacji w koncie lokalnym do konta domenowego.

6. Wraz z rozwiązaniem serwerowym musi zostać dostarczone 30 licencji oprogramowania do szyfrowania komputerów i pamięci zewnętrznej wraz z wsparciem technicznym i prawem do aktualizacji na 2 lata o następujących parametrach:

6.1. Oprogramowanie musi zapewnić możliwość centralnego zarządzania systemem szyfrowania i jego konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność:

6.1.1. wyświetlać komputery wraz z dyskami systemowymi oraz dyskami podłączonymi do komputera

6.1.2. umożliwiać włączenie szyfrowania na wybranych dyskach

6.1.3. możliwość szyfrowania dysków systemowych

6.1.4. szyfrowanie/deszyfrowanie dysków w trakcie pracy użytkownika na komputerze

6.1.5. wyświetlać zbiorcze raporty, które komputery są szyfrowane, a które nie

6.1.6. wyświetlać zdarzenia, jakie są wykonywane podczas szyfrowania:

6.1.6.1. postęp szyfrowania/deszyfrowania

6.1.6.2. logi z wykonywanych operacji zapisane w centralnej bazie

6.1.7. wyświetlać listę dysków jakie były podłączane do komputerów

6.2. Oprogramowanie instalowane na komputerze musi zapewnić funkcjonalność:

6.2.1. umożliwiać zdalną instalację agentów na wybranych komputerach

6.2.2. umożliwiać instalację oprogramowania w trybie cichym bez ingerencji użytkownika

6.2.3. wspierać dyski HDD i SSD

6.2.4. umożliwiać szyfrowanie dysków lokalnych i wymiennych FAT32, NTFS algorytmem AES

6.2.5. wspierać systemy Windows 7, 8, 8.1, 10, 11 w wersji pro i home

6.2.6. system musi informować użytkownika o postępie szyfrowania dysku

6.2.7. system musi wznawiać szyfrowanie dysku w przypadku resetu, wyłączenia lub zawieszenia komputera

6.2.8. system musi poinformować użytkownika o procesie szyfrowania w momencie gdy użytkownik będzie chciał go poprawnie wyłączyć lub zrestartować. Aplikacja powinna oprócz takiego poinformowania dać możliwość wyboru użytkownikowi czy system sam automatycznie ma się wyłączyć po zakończeniu szyfrowania, czy też nie

6.3. Licencja oprogramowania musi być licencją bezterminową na użytkowanie z dwuletnim wsparciem technicznym i prawem do aktualizacji.

7. Na zaoferowane w punktach 1-6 oprogramowanie wymagane jest zapewnienie wsparcia technicznego i prawa do aktualizacji na 24 miesiące.

Specyfikacja wdrożenia:

1. Wykonawca do wdrożenia oferowanych rozwiązań musi posiadać następujące osoby z uprawnieniami:

1.1 jedną osobę posiadającą uprawnienia Audytora Wiodącego ISO 27001:2013 i Audytora Wewnętrznego ISO 14001 i 50001 lub uprawnienia równoważne,

1.2 jedną osobę posiadającą uprawnienia Audytora Wewnętrznego ISO 27001:2013 i MCSA SQL Server 2012 i MCSA Windows Server 2012 lub uprawnienia równoważne.

2. Wdrożenie obejmuje dostarczenie sprzętu do miejsca docelowego, instalację sprzętu oraz jego konfigurację. Dopuszcza się konfigurację zdalną.

3. W ramach wdrożenia wykonawca przeszkoli kadrę informatyczną Urzędu z wdrożonych rozwiązań. Osoba szkoląca musi posiadać uprawnienia Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne.

Część 10

3 sztuki wysokowydajnych urządzeń wielofunkcyjnych, mogących pełnić funkcję drukarki sieciowej, skanera sieciowego oraz kopiarki, z funkcjonalnością drukowania zabezpieczonego kodem PIN

<u>Specyfikacja pojedynczego urządzenia:</u>

Przedmiotem zamówienia jest zakup nowoczesnego, wysokowydajnego urządzenia wielofunkcyjnego, mogącego pełnić funkcję drukarki sieciowej, skanera sieciowego oraz kopiarki, z funkcjonalnością drukowania zabezpieczonego kodem PIN.

- drukowanie i kopiowanie A4, A3 w kolorze,
- dupleks strumieniowy (do 200g),
- prędkość drukowania/kopiowania minimum 35 stron A4/min. zarówno w trybie czarno-białym oraz kolorowym,
- obsługiwana gramatura papieru do 300g/m2
- min. 2 kasety na 500 arkuszy + podajnik ręczny na 100 arkuszy,
- zewnętrzny finiszer dwupółkowy z opcją zszywania wydruków,
- RDF (jednoprzebiegowy automatyczny podajnik dokumentów dwustronnych) na minimum 150 arkuszy z prędkością pobierania min. 100 stron A4/min.,
- kolorowy skaner PDF, PDF szyfrowany, PDF OCR, TIF, JPEG, Word OCR do komputera (serwer SMB) lub e-maila,
- sieciowy skaner kolorowy TWAIN współpracujący z OCR,
- skanowanie i drukowanie do/z nośnika pamięci zewnętrznej,
- funkcjonalność poufnych skrzynek pocztowych dla min. 100 użytkowników do zapisywania zeskanowanych dokumentów na dysku twardym urządzenia i drukowanie ich na żądanie, dostęp do skrzynek za pomocą hasła o min. 8 znakach, przechowywanie plików do 30 dni,
- wydruk zabezpieczony kodem dostępu (kody podzielone na wydziały, osoby),
- karta sieciowa RJ-45,
- port USB 2.0,
- pamięć graficzna drukarki i kopiarki min. 4 GB RAM, przestrzeń na twardym dysku min. 250 GB,
- kolorowy pulpit sterowniczy z wyświetlaczem ciekłokrystalicznym min. 10 cali,
- zarządzanie urządzeniem w jęz. polskim,
- instrukcja obsługi urządzenia w jęz. polskim,
- sterownik drukarki UFR/PCL/PS Windows 7/8/10/11 w języku polskim,
- sterownik skanera TWAIN

Dopuszczalne jest dostarczenie urządzeń poleasingowych o maksymalnym przebiegu: 200 tys. wydruków czarno-białych / 100 tys. wydruków kolorowych.

Gwarancja:
- gwarancja 36 miesięcy,
- zapewnienie serwisu gwarancyjnego i pogwarancyjnego (zwłaszcza w przypadku dostarczenia urządzeń poleasingowych).