UG.271.12.2022

Załącznik nr 7 do SWZ

Szczegółowy opis przedmiotu zamówienia

1. 4 szt. komputerów przenośnych w konfiguracji:

Nazwa	Wymagane minimalne parametry techniczne
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej,
Matryca	Komputer przenośny typu notebook z ekranem dotykowym 14,0" o rozdzielczości FHD (1920 x 1080) z technologią panelu wyświetlacza WVA, z technologią TrueLife,
Procesor	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 11000 punktów według wyników ze strony https://www.cpubenchmark.net
Pamięć RAM	16GB DDR4 3200 MHz , dwa sloty pamięci
Pamięć masowa	min. 512 GB SSD NVMe
Karta graficzna	Zintegrowana z procesorem Odrębna karta graficzna posiadająca minm 2 GB pamięci VRAM GDDR5
Multimedia	Dwukanałowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy min. 2x 2W, dwa mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa o rozdzielczości min. HD trwale zainstalowana w obudowie matrycy.
Bateria i zasilanie	Bateria 3-ogniowa. Zasilacz o mocy min. 65W. Konstrukcja komputera musi umożliwiać demontaż samej baterii lub wszystkich zainstalowanych baterii, samodzielnie bez udziału serwisu w okresie gwarancyjnym. Bateria nie może być trwale zespolona z płytą główną.
Waga	Waga komputera z oferowaną baterią nie większa niż 1,7 kg
Obudowa	Obudowa notebooka wzmocniona, szkielet i zawiasy notebooka wykonany z wzmacnianego metalu.

BIOS	BIOS zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy. BIOS musi umożliwiać przeprowadzenia inwentaryzacji sprzętowej poprzez wyświetlenie informacji o: wersji BIOS, numerze seryjnym i dacie produkcji komputera, wielkości, prędkości i sposobie obsadzenia zainstalowanej pamięci RAM, typie zainstalowanego procesora, zainstalowanym dysku twardym (pojemność, model), MAC adresie wbudowanej w płytę główną karty sieciowej.

	Funkcja blokowania/odblokowania portów USB Możliwość, ustawienia hasła dla administratora oraz użytkownika dla BIOS'u, po podaniu hasła użytkownika możliwość jedynie odczytania informacji, brak możliwości wł/wy funkcji. Hasła silne opatrzone o litery, cyfry i znaki specjalne. Możliwość przypisania w BIOS numeru nadawanego przez Administratora.
Bezpieczeństwo	System diagnostyczny z graficzny interfejsem dostępny z poziomu BIOS lub menu BOOT'owania umożliwiający użytkownikowi przeprowadzenie wstępnej diagnostyki awarii poprzez przetestowanie: procesora, pamięci RAM, dysku, płyty głównej i wyświetlacza. Pełna funkcjonalność systemu diagnostycznego musi być dostępna również w przypadku braku lub uszkodzenia oraz sformatowania dysku twardego, braku dostępu do sieci LAN i internetu oraz nie może być realizowana przez narzędzia zewnętrzne podłączane do komputera (np. pamięć USB flash]. Dedykowany układ szyfrujący TPM Mechaniczna osłona kamery, czytnik linii papilarnych.
Certyfikaty (Wykonawca, którego oferta zostanie wybrana, jako najkorzystniejsza zobowiązany jest dołączyć przed podpisaniem umowy)	Deklaracja zgodności CE Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.
System operacyjny	Zainstalowany system operacyjny Windows 11 Home

Wymagania dodatkowe	Wbudowane porty i złącza: HDMI 1.4, min. 2 port USB 3.2 gen1 typ-A, USB Typu-C (z DisplayPort i Power Delivery), czytnik kart microSD, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, złącze zasilania (zasilacz nie może zajmować portów USB) Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11AC, moduł bluetooth 4.1 Klawiatura z wbudowanym podświetleniem (układ US - QWERTY), touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów. Laptop musi posiadać możliwość ustawienia w pozycji tableta.
Dodatkowe oprogramowanie	Dostarczone i zainstalowane w środowisku systemu operacyjnego aplikacja zapewniająca bezproblemową integrację bezprzewodową między smartfonami i komputerem. Aplikacja wspierająca zgodna z systemami iOS oraz Android 6 lub nowszy. Opatrzona w funkcjonalności: - Inicjowanie i odbieranie połączeń telefonicznych przez głośniki i mikrofon w komputerze
	- Uzyskanie dostępu do kompletnej książki telefonicznej poprzez komputer - Wysyłanie i odbieranie wiadomości tekstowych za pomocą klawiatury, myszy i ekranu dotykowego komputera. - bezprzewodowo: przeciągnij i upuść zdjęcia, filmy, muzykę i dokumenty między komputerem a smartfonem z systemem Android lub iOS. - tworzenie kopi lustrzanej ekranu telefonu z systemem Android lub iOS na komputerze i korzystanie z dowolnych aplikacji za pomocą klawiatury, myszy i ekranu dotykowego komputera
Warunki gwarancji	36 miesięczna gwarancja producenta świadczona na miejscu u klienta (on-site). Czas reakcji serwisu - do końca następnego dnia roboczego. Możliwość dedykowanego portalu producenta do zgłaszania awarii lub usterek, możliwość samodzielnego zamawiania zamiennych komponentów oraz sprawdzenie okresu gwarancji, fabrycznej konfiguracji. Firma serwisująca posiadać autoryzacje producenta komputera.

2. 2 szt. serwerów + system operacyjny w konfiguracji:

Obudowa	• Typu RACK, wysokość nie więcej niż 1U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej; • Ramię porządkujące przewody z tyłu serwera;
Płyta główna	• Dwuprocesorowa; • Wyprodukowana i zaprojektowana przez producenta serwera • Możliwość instalacji procesorów 28-rdzeniowych; • Zainstalowany moduł TPM 2.0 • 4 złącza PCI Express generacji 3 w tym: o 3 fizyczne złącza o prędkości x16; o 1 fizyczne złącze o prędkości x8;
	o Możliwość rozbudowy o riser umożliwiający instalację kart full height • 24 gniazda pamięci RAM; • Obsługa minimum 3TB pamięci RAM; • Wsparcie dla technologii: o Memory Scrubbing o SDDC o Advanced ECC o Rank Sparing; • Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM o pojemności sumarycznej minimum 1TB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) • Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;
Procesory	• 2 procesory 8-rdzeniowe • architektura x86 • Taktowanie bazowe 2,1GHz • Osiągający w oferowanym serwerze w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 93 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów w oferowanym serwerze).

Pamięć RAM	• 128GB (8x16GB) pamięci RAM • DDR4 Registered • 2933Mhz
Dyski twarde i napędy	• Minimum 8 wnęk dla dysków twardych Hotplug 2,5”; • Zainstalowane 2 dyski SSD 480GB Hot Plug DWPD>3,5; • Możliwość instalacji wewnętrznej nagrywarki Blu-Ray;
Kontrolery LAN	• Zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 6x 1Gbit Base-T • Dodatkowa karta 4x 10Gbit Base-T;
Kontrolery I/O	• Zainstalowany kontroler SAS RAID obsługujący poziomy: 0,1,10,5,50; • Możliwość zainstalowania 2 nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug
Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; • 2 port USB 3.0 na panelu przednim; • 1 port USB 3.0 wewnętrzny; • 2 porty USB 3.0 dostępne z tyłu serwera; • Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;
Zasilanie, chłodzenie	• Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 800W; • Redundantne wentylatory hotplug;

Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii) o informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: ✦ karty rozszerzeń zainstalowane w dowolnym slocie PCI Express ✦ procesory CPU ✦ pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM ✦ wbudowany na płycie głównej nośnik pamięci M.2 SSD ✦ status karty zrządzającej serwera ✦ wentylatory ✦ bateria podtrzymująca ustawienia BIOS płyty główne ✦ zasilacze System przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym); Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ○ Dostęp poprzez przeglądarkę Web, SSH; o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; ○ Zarządzanie alarmami (zdarzenia poprzez SNMP) o Możliwość przejęcia konsoli tekstowej o Możliwość zarządzania przez 2 administratorów jednocześnie o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)

	○ Obsługa serwerów proxy (autentykacja) ○ Obsługa VLAN o Możliwość konfiguracji parametru Max. Transmission Unit (MTU) o Wsparcie dla protokołu SSDP o Obsługa protokołów TLS 1.2, SSL v3 ○ Obsługa protokołu LDAP o Integracja z HP SIM ○ Synchronizacja czasu poprzez protokół NTP ○ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);

	• Dedykowana lub wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
Wspierane OS	• Microsoft Windows Server 2019, 2016 • VMWare vSphere 6.7, 6.5 • Suse Linux Enterprise Server 12 • Red Hat Enterprise Linux 7, 8 • Oracle Linux 7 • Oracle VM 3
Gwarancja	• 60 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika do końca następnego dnia roboczego od zgłoszenia. Naprawa realizowana przez producenta lub certyfikowanego serwisanta. • Automatyczne zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; • Dyski twarde nie podlegają zwrotowi organizacji serwisowej; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie on-site z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki
Dokumentacja, inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE

	• Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, Wykonawca, którego oferta zostanie wybrana, jako najkorzystniejsza zobowiązany jest dołączyć przed podpisaniem umowy zobowiązany jest do podania linku do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
	• Możliwość bezpłatnej aktualizacji i bezpłatnego pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

Udzielona, nieograniczona czasowo i terytorialnie bezpłatna licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie nielimitowanej ilości instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18) Mechanizmy logowania w oparciu o:
   a) Login i hasło,
   b) Karty z certyfikatami (smartcard),
   c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
   b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
      i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
      ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
      iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
      iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
   c) Zdalna dystrybucja oprogramowania na stacje robocze.
   d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
   e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
      i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
   f) Szyfrowanie plików i folderów.
   g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
   h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
   i) Serwis udostępniania stron WWW.
   j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
   k) Wsparcie dla algorytmów Suite B (RFC 4869),
   l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
   m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
iii. Obsługi 4-KB sektorów dysków
iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

3. 25 szt. stacji roboczych w konfiguracji:

Podzespół	Minimalne parametry
1. Typ komputera	**Komputer stacjonarny**
2. Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do zasobów lokalnej sieci komputerowej oraz usług sieci Internet, aplikacji graficznych wektorowych oraz rastrowych, a także danych multimedialnych.
3. Procesor	klasy x86, 6 rdzeniowy, ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych, zapewniający wydajność min. 12200 pkt. w teście Passmark CPU Mark, znajdujący się na liście https://www.cpubenchmark.net/cpu_list.php

4. Płyta główna	- chipset dostosowany do oferowanego procesora lub równoważny - minimum 4 sloty pamięci 3200 MT/s - minimum 1 x PCI Express 4.0 x 16 - minimum 1 x PCI Express 3.0 x 4 - minimum 5 złącz SATA 6.0 Gb/s

	- minimum 1x M.2 dla dysku SSD o przepustowości 64Gbit/s - minimum 1x M.2 dla dysku SSD o przepustowości 32Gbit/s - 1x USB (gniazdo bezpośrednio na płycie głównej)
5. Pamięć operacyjna RAM	- minimum 8GB GB DDR4 - minimalny rozmiar możliwego rozszerzenia obsługiwanej pamięci, zapewniony i potwierdzony przez producenta komputera: 128 GB
6. Porty w tylnej części komputera	Komputer musi posiadać: - minimum 2 x Display Port 1.4 z obsługą funkcji Multi-Stream, - możliwość zainstalowania trzeciego interfejsu wideo bez konieczności dokładania zewnętrznych kart graficznych; - minimum 6 x USB, w tym co najmniej 2x USB 3.2 Gen 1 - minimum 1 port sieciowy RJ-45, - Możliwość wyprowadzenia 1x port szeregowy (RS-232) – opcja rozbudowy, - osobne porty audio line-in i line-out Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB oraz VIDEO nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
6. Porty w przedniej części komputera	Komputer musi posiadać: - minimum 4 x USB-A, w tym min. 1x USB 3.2 Gen 2 - minimum 1 x USB -C 3.2 Gen 2 z obsługą Display port i Power Delivery - port audio do podłączenia słuchawek z mikrofonem
7. Dysk twardy	- Minimum 256GB SSD z interfejsem M.2 NVMe, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego zainstalowanego na komputerze przez producenta, po awarii, do stanu fabrycznego (tryb OOBE dla systemu MS Windows) - Dodatkowy dysk wewnętrzny minimum 1000GB SATA.

8. Napęd optyczny	Nagrywarka DVD +/-RW
9. Karta dźwiękowa	Karta dźwiękowa zintegrowana z płytą główną, zgodna ze standardem High Definition 5.1
10. Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Pełna obsługa funkcji i standardów DX12, OpenGL 4.5, OpenCL 2.1. Możliwość fabrycznego zainstalowania dodatkowej, dedykowanej karty graficznej z pamięcią własną min. 4 GB. Grafika zintegrowana w procesorze musi umożliwiać jednoczesną obsługę co najmniej trzech monitorów. Na potrzeby obsługi większej liczby monitorów oferowany komputer musi
	umożliwiać jednoczesną obsługę monitorów podłączonych do grafiki zintegrowanej w procesorze oraz zainstalowanej osobnej karty graficznej (jeśli jest ona wymagana).
11. Karta sieciowa	Karta sieciowa 10/100/1000 Ethernet RJ-45, zintegrowana z płytą główną wspierająca obsługę technologii WoL oraz PXE. Zintegrowana karta sieciowa musi być wyposażona w diodę statusu informującą a aktywności połączenia oraz diodę informującą o prędkości połączenia.

12. BIOS	**BIOS UEFI w wersji 2.6 lub wyższej. Możliwość odczytania z BIOS informacji o:** - modelu komputera, - numerze seryjnym, - AssetTag/IDTag - MAC Adres karty sieciowej, - wersja Biosu wraz z datą jego produkcji, - zainstalowanym procesorze, jego taktowaniu - ilości pamięci RAM wraz z taktowaniem i obłożeniem slotów **Możliwość z poziomu BIOS:** - wyłączenia selektywnego portów USB, minimum wyłączanie portów z przodu oraz wyłączanie portów z tyłu jako grup - wyłączenia selektywnego (pojedynczego) portów SATA, - zmiany pracy wentylatorów między trybem optymalizacji głośności lub temperatury, - ustawienia hasła: administratora, Power-On, HDD, - możliwość zbierania i przeglądania logów zdarzeń z informacją odnośnie godziny, daty i kodu błędu zdarzenia - ustawienie automatycznej aktualizacji BIOS z serwera producenta komputera
13. Klawiatura	Klawiatura USB w układzie polskim programisty (105 klawiszy) z kablem o długości min. 1,8 m.
14. Mysz	Mysz optyczna USB z klawiszami oraz rolką (scroll) z kablem o długości min. 1,8 m.
15. Obudowa	- Typu desktop (SFF) przystosowana do pracy w pionie i w poziomie, z obsługą kart PCI Express wyłącznie o niskim profilu;. - Wbudowany głośnik do odtwarzania plików multimedialnych. - Suma wymiarów obudowy, nie może przekroczyć: 700 mm, najkrótszy z wymiarów nie większy niż: 90 mm

	- Czujnik otwarcia obudowy współpracujący z oprogramowanie do monitorowania stanu otwarcia obudowy. Fakt otwarcia obudowy musi być odnotowany w logach w BIOS; - Możliwość zainstalowania wewnętrznego filtra przeciwkurzowego; - Obudowa jednostki centralnej beznarzędziowa, pozwalająca na demontaż komponentów i kart rozszerzeń (PCIe) oraz napędu optycznego i dysków twardych (co najmniej 3,5 cala) bez użycia narzędzi, z obiegiem powietrza tylko przód-tył - brak perforacji na bokach obudowy . - Głośność jednostki centralnej nie może przekraczać 18 dB, mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie czuwania (tryb Idle). Wymagany raport badawczy, wystawiony przez niezależną, akredytowaną, co najmniej dla norm ISO 7779 i ISO 9296 jednostkę badawczą lub wpis w karcie katalogowej producenta komputera
16. Zasilanie	Zasilacz o mocy min 280 W pracy ciągłej i sprawności min. 92% przy obciążeniu 50%. Zasilacz komputera jest wyposażony w gniazdo umożliwiające podłączenia zasilania do monitora

17. Bezpieczeństwo i funkcje zarządzania	1. Możliwość zastosowania mechanicznego zabezpieczenia przed kradzieżą komputera. 2. TPM 2.0. 3. Możliwość wbudowania czytnika SmartCard 4. Certyfikowane oprogramowanie umożliwiające – bez względu na stan czy obecność systemu operacyjnego w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego metodą 35 przebiegową - w ofercie należy podać nazwę i producenta oprogramowania. 5. System diagnostyczny działający bez udziału systemu operacyjnego, czy też jakichkolwiek dołączonych urządzeń na zewnątrz czy też wewnątrz komputera, umożliwiający otrzymanie informacji o: - modelu, oznaczeniu i numerze seryjnym komputera, pojemności zainstalowanej pamięci RAM **Oprogramowanie diagnostyczne musi umożliwiać:** - wykonanie testu pamięci RAM, - wykonanie podstawowego testu prawidłowej pracy CPU - wykonanie testu dysku twardego. System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera (Zaimplementowany w sprzętowym mikrokodzie płyty głównej)

18. Sterowniki i oprogramowanie	Zapewnienie bezpłatne na dedykowanej stronie internetowej producenta dostępu do najnowszych sterowników i uaktualnień, realizowane poprzez podanie numeru seryjnego/modelu urządzenia, podać link strony www. Oprogramowanie producenta komputera posiadające funkcje zarządzania sterownikami (wykrywanie i instalowanie aktualizacji). Oprogramowanie umożliwiające – bez względu na stan czy obecność systemu operacyjnego oraz bez podłączania żadnych urządzeń czy nośników zewnętrznych - w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego. Usuwanie danych z dysku twardego musi odbywać się przy wykorzystaniu certyfikowanych algorytmów a wynikiem pracy oprogramowania musi być protokół zawierający dane kasowanego dysku oraz informacje o zastosowanym algorytmie kasowania.

19. Certyfikaty i oświadczenia	1. Oferowane komputery stacjonarne muszą posiadać europejską deklarację zgodności CE. 2. Certyfikat poprawnej współpracy z zaoferowanym systemem operacyjnym (wydruk ze strony producenta oprogramowania systemowego). 3. Certyfikat Energy Star 8.0, 4. Epeat Silver. Wykonawca, którego oferta zostanie wybrana, jako najkorzystniejsza zobowiązany jest dołączyć przed podpisaniem umowy zobowiązany jest do podania linku do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki
20. Zainstalowane oprogramowanie systemowe	Zainstalowany system operacyjny co najmniej Windows 10 Pro 64-bitowy w polskiej wersji językowej lub system równoważny wraz z nośnikiem instalacyjnym. Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego. *Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.* System równoważny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

	1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim. 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 4. Wbudowany system pomocy w języku polskim. 5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. 8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. 9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.


Fundusze
Europejskie
Polska Cyfrowa


Rzeczpospolita
Polska


Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

	17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. 18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 22. Obsługa standardu NFC (near field communication). 23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 26. Mechanizmy logowania do domeny w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 27. Mechanizmy wieloelementowego uwierzytelniania. 28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. 30. Wsparcie dla algorytmów Suite B (RFC 4869). 31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. 32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.

	35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,

	36. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 40. Udostępnianie modemu. 41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 43. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. 46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. 49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

21. Gwarancja – zgodnie z wymaganiami i kryteriami	• 60 miesięcy świadczonej w siedzibie Zamawiającego, przyjazd certyfikowanego przez producenta serwisanta do końca następnego dnia roboczego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca. • Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta • Uszkodzone dyski nie podlegają zwrotowi organizacji serwisowej • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela

4. 29 Licencji Microsoft Office Home & Business 2021 PL

• Wersja BOX
• Zawiera programy Word, Excel, PowerPoint i Outlook na system Windows 10
• Jednorazowy zakup instalowany na 1 komputerze PC lub Mac.
• Uwzględniona pomoc techniczna firmy Microsoft przez 60 dni bez dodatkowych kosztów
• Wersja językowa – polska
• Czas trwania – licencja wieczysta

5. Macierz blokowa pozwalająca na wykorzystanie jej jako wspólna przestrzeń pod wirtualizację (np. Vmware, Citrix, HyperV), dedykowane rozwiązanie dla wymagających aplikacji (SQL, Oracle, Exchange), lub przestrzeń dla przechowywania kopii zapasowych i archiwów.

Nazwa	Wymagane minimalne parametry techniczne
Obudowa wysokość	2U
Szerokość	19”, obudowa mieszcząca min 24 dyski 2,5’’
Prędkość obrotowa dysków	min 10 tysięcy RPM

Pamięć Cache	min 16GB Cache
Serwis	Dostawa części NextBusinessDay + Subskrypcja do oprogramowania + dostęp do baz wiedzy i portalu serwisowych na 36 miesięcy
Macierz blokowa, wspiera połączenia	FC, iSCSI, SAS
W cenie macierzy funkcjonalności	Szybka odbudowa dysków RAID, Partycjonowanie, ThinProvisioning, RAID Level Migration, SSD Cache, Snapshoty, Replikacja
Liczba kontrolerów	Min 2
Zainstalowane Porty	min 4x12Gb SAS, 8x25GbE (w zestawie wkładki 10GbE SFP+)
Dodatkowe	Zainstalowane oprogramowanie do zarządzania Automatyczne i proaktywne wsparcie

6. Urządzenie UTM

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 Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
5. 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.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
7. 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**
13. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. 3. 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.
15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS). • Microsoft Azure
    - Google Cloud Platform (GCP).
    - OpenStack.
    - VMware NSX.

Połączenia VPN

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

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

Routing i obsługa łączy WAN

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

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

Kontrola aplikacji

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

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

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

Zarządzanie

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

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

• ICSA lub EAL4 dla funkcji Firewall - Wykonawca, którego oferta zostanie wybrana, jako najkorzystniejsza zobowiązany jest dołączyć przed podpisaniem umowy.

Serwisy i licencje

Wykonawca, którego oferta zostanie wybrana, jako najkorzystniejsza zobowiązany jest dołączyć przed podpisaniem umowy 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 36 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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.

Opisy do wymagań ogólnych

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

7. Urządzenie do tworzenia kopii zapasowych i ochrony danych

Nazwa	Minimalne wymagania
Procesor	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 10000 punktów

	według wyników ze strony https://www.cpubenchmark.net
Architektura procesora	64-bitowy x86
RAM	min 8 GB DDR4 (1 x 8 GB)
Maksymalna pojemność pamięci	64 GB (2 x 32 GB)
Ilość gniazd RAM	2 x SO-DIMM DDR4, wsparcie dla pamięci ECC
Pamięć flash	min 5 GB (ochrona systemu operacyjnego przed podwójnym rozruchem)
Wnęka dysków	Wnęka musi pomieścić min 8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s. Dyski muszą mieć możliwość wymiany podczas pracy urządzenia.
M.2 Slot	Wymagana obecność 2 slotów M.2
Port 2,5 Gigabit Ethernet (2,5G/1G/100M)	Obecność min 2 Portów 2,5 Gigabit Ethernet (2,5G/1G/100M)
Port 5 Gigabit Ethernet (5G/2,5G/1G/100M)	Możliwość zamontowania portów 5 Gigabit Ethernet (2,5G/1G/100M) poprzez kartę PCIe
Port 10 Gigabit sieci Ethernet	Możliwość zamontowania portów 10 Gigabit sieci Ethernet poprzez kartę PCIe
Gniazdo PCIe	Gniazdo 1: PCIe Gen 3 x4 Gniazdo 2: PCIe Gen 3 x4
Port USB	Urządzenie wyposażone w 3 wejścia Typu-A USB 3.2 Gen 2 10Gbps Urządzenie wyposażone w 1 wejście Typu-C USB 3.2 Gen 1 5Gbps
Typ urządzenia	Tower
Zasilacz	250 W, 100–240 V
Wentylator	Wentylator systemu: 2 x 120 mm Wentylator procesora: 1 x 60 mm

Dodatkowe funkcjonalności	Możliwość zamontowania procesora graficznego poprzez kartę PCIe Obecność koprocesora arytmetycznego FPU, Mechanizmu szyfrowania Opcjonalne poprzez kartę PCIe Transkodowanie wspomagane sprzętowo Obsługa przyspieszenia pamięci podręcznej SSD Zamontowany element do ostrzegania systemowego Zamontowane złącze bezpieczeństwa

8. Urządzenia wielofunkcyjne posiadające funkcjonalność kopiarki, drukarki, skanera, faksu o parametrach:

OGÓLNE	
Czas nagrzewania	Max 18 sekund
Prędkość wykonania pierwszego wydruku: mono	Max 4,1 sekundy
Prędkość wydruku ciągłego	Minimum 25 str.na min.
Pamięć: maksymalnie	2 GB
Dysk twardy: maksymalnie	320 GB
Pojemność ARDF	Min 100 arkuszy
Pojemność SPDF	Min 220 arkuszy
Źródło zasilania	220 - 240 V,
KOPIARKA	
Kopiowanie wielokrotne	Do 999 kopii
Rozdzielczość: maksymalnie	Min 600 dpi
Zoom	Od 25% do 400% w krokach co 1%
DRUKARKA	
Procesor	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 1900 punktów

	według wyników ze strony https://www.cpubenchmark.net
Język drukarki: standardowo	PCL5e, PCL6, PostScript 3 (emulacja), PDF Direct (emulacja)
Język drukarki: opcja	Adobe® PostScript®3™, IPDS, PDF Direct od Adobe®
Rozdzielczość wydruku: maksymalnie	Min 1 200 x 1 200 dpi
Interfejs: standardowo	Ethernet 10 base-T/100 base-TX/1000 base-T, Interfejs hosta USB Typ A, Interfejs urządzenia z USB Typ B
Interfejs: opcja	Dwukierunkowy IEEE 1284/ECP, Bezprzewodowa sieć LAN (IEEE 802.11a/b/g/n), Dodatkowa karta sieciowa (drugi port)
Możliwość druku mobilnego	Poprzez Apple AirPrint, Mopria®, NFC, Ricoh Smart Device Connector
Środowiska Windows®	Windows® 8.1, Windows® 10, Windows® Server 2012, Windows® Server 2012R2, Windows® Server 2016, Windows® Server 2019
Środowiska Mac OS	Macintosh OS X v10.13 lub nowsze

SKANER

Prędkość skanowania: ARDF	Minimum 80 obrazów na minutę (200/300 dpi)
Prędkość skanowania: SPDF	Minimum 120 obrazów na minutę (jednostronnie)/240 obrazów na minutę (dwustronnie)
Rozdzielczość: maksymalnie	600 dpi
Formaty pliku	Jednostronicowy TIFF, Jednostronicowy JPEG, Jednostronicowy PDF, Jednostronicowy PDF wysoki poziom kompresji, Jednostronicowy PDF-A, Wielostronicowy TIFF, Wielostronicowy PDF, Wielostronicowy PDF wysoki poziom kompresji, Wielostronicowy PDF-A
Tryby skanowania	E-mail, USB, Karta SD, Adres URL, FTP, SMB

FAKS

Sieć	PSTN, PBX

Prędkość transmisji	Min 2 sekundy
Prędkość modemu: maksymalnie	33,6 kb⁄s
Rozdzielczość: standardowo	Min 8x3,85 linia/mm, 200x100 dpi, 8x7,7 linia⁄mm, 200x200 dpi
Rozdzielczość: opcja	Min 16x15,4 linia/mm, 400x400 dpi
Metoda kompresji	MH, MR, MMR, JBIG
Pamięć: standardowo	Min 4 MB, (ok. 320 stron)
Pamięć: maksymalnie	Min 60 MB, (ok. 4 800 stron)
OBSŁUGIWANY PAPIER	
Zalecany rozmiar papieru - Standardowa/e kaseta/y na papier:	A3, A4, A5, A6, B4, B5, B6, Koperty
Zalecany rozmiar papieru - Opcjonalna kaseta na papier:	A3, A4, A5, A6, B4, B5, B6, Koperty
Zalecany rozmiar papieru - Taca ręczna:	A3, A4, A5, A6, B4, B5, B6, Koperty, Niestandardowy rozmiar papieru
Pojemność wejściowa: standardowo kasety	Min 1 200 arkuszy
Pojemność wejściowa: maksymalnie	4 700 arkuszy
Pojemność wyjściowa: standardowo	500 arkuszy
Pojemność wyjściowa: maksymalnie	1 625 arkuszy
Typy papieru	Papier zwykły, Papier ekologiczny, Papier specjalny, Papier kolorowy, Papier firmowy, Karty, Papier z nagłówkiem, Papier dokumentowy, Papier powlekany, Koperty, Papier na etykiety, Folia przezroczysta
EKOLOGIA	

Zużycie energii: maks.	1 600W
Współczynnik TEC (kWh)*	0,29 kWh/tydzień

OPCJE TAC WYJŚCIOWYCH I FINISHERA	
1 x 550-arkuszowa kaseta na papier - Rozmiar papieru:	A3, A4, A5, A6, B4, B5, B6
2 x 550-arkuszowa kaseta na papier - Rozmiar papieru:	A3, A4, A5, A6, B4, B5, B6
2 x 550-arkuszowa kaseta na papier - Gramatura papieru:	60-300 g/m²
2,000-arkuszowa kaseta o dużej pojemności - Rozmiar papieru:	A4
2,000-arkuszowa kaseta o dużej pojemności - Gramatura papieru:	60-300 g/m²
1,500-arkuszowa boczna kaseta o dużej pojemności - Rozmiar papieru:	A4, B5
1,500-arkuszowa boczna kaseta o dużej pojemności - Gramatura papieru:	60-300 g/m²
Hybrydowy finiszer na 1 000 arkuszy - Rozmiar papieru:	SRA3, A3, A4, A5, A6, B4, B5, B6
Hybrydowy finiszer na 1 000 arkuszy - Gramatura papieru:	52-300 g/m²
Hybrydowy finiszer na 1 000 arkuszy	1 000 arkuszy

Hybrydowy finiszer na 1 000 arkuszy - Pojemność zszywacza:	50 arkuszy
Hybrydowy finiszer na 1 000 arkuszy - Rozmiar zszywanego papieru:	A3, A4, B4, B5
Hybrydowy finiszer na 1 000 arkuszy - Gramatura zszywanego papieru	52-105 g/m²
Hybrydowy finiszer na 1 000 arkuszy - Pozycja zszywania:	Góra, dół , 2 zszywki
Rozmiar papieru:	A3, A4, A5, A6, B4, B5, B6, A3, A4, A5, A6, B4, B5, B6
Gramatura papieru:	52-300 g/m², 52-300 g/m²
Pojemność:	3 000 arkuszy, 2 000 arkuszy
Pojemność zszywacza:	50 arkuszy, 50 arkuszy
Rozmiar zszywanego papieru:	A3, A4, B4, B5, A3, A4, B4, B5
Gramatura zszywanego papieru	52-105 g/m², 52-105 g/m²
Pozycja zszywania:	Góra, Dół, 2 zszywki, Góra ukośnie, Góra, Dół, 2 zszywki, Broszura
MATERIAŁY EKSPLOATACYJNE	
Toner: czarny	24 000 wydruków

9. Przedłużenie posiadanych licencji antywirusa ESET Endpoint Antivirus na rok:

Licencja źródłowa:

ESET Endpoint Antivirus / Ważna do dnia: **2023-05-03** / Obecna liczba stanowisk: **82**

Licencja docelowa:

ESET Endpoint Antivirus / Docelowa liczba stanowisk: **82**

10. Stworzenie strony WWW Urzędu

Opracowanie kompleksowej kreacji graficznej Serwisu WWW	• Stworzenie projektu graficznego • Na stronie głównej znajdzie się:Menu/Podstrony, grafika, zdjęcia • Projekt będzie nawiązywał do specyfiki branży oraz proflu działalności instytucji • Projekt wpisujący się w najnowsze trendy w Internecie • Projekt zgodny z wytycznymi Klienta omówionymi szczegółowo na spotkaniu • Intuicyjna nawigacja serwisu ułatwiająca użytkownikowi swobodne poruszanie się po serwisie • Przejrzysta struktura, przejrzysty podział treści minimalizujący liczbę WYJŚĆ ze strony
Możliwość samodzielnej obsługi strony	• Dodawanie , usuwanie zdjęć, tekstów, plików • Obsługa panelu bardzo intuicyjna (tak jak w Wordzie) • Możliwość nadawania uprawnień poszczególnym pracownikom, którzy będą administrować serwisem • Możliwość rozbudowy Menu o dodatkowe zakładki

	• Możliwość załączenia plików multimedialnych np.: filmów • Strona dostępna zgodnie ze standardem WCAG 2.1

Specyfikacja serwisu	• atrakcyjny design • nowoczesna i użyteczna forma graficzna opcjonalnie uzupełniona w animowane elementy • Content Managment System – system zarządzania treścią służący do zarządzania serwisami z możliwością obsługi przez kilku użytkowników • serwisy zintegrowane w nowoczesny, intuicyjny system tak aby istniała możliwość jego późniejszej rozbudowy • serwisy w kilku wersjach językowych (opcjonalnie) • zgodne z obowiązującymi standardami i poziomem artystycznym obowiązującym na rynku • zastosowanie różnych technologii dobranych do wymogów danej realizacji, (Flash, XHTML, AJAX, PHP, PostgreSQL, MySQL lub podobnych) • zastosowanie technolgii Responsive Web Design (RWD) – wygląd i układ dostosowuje się automatycznie do rozmiaru okna przeglądarki • Strony zbudowane zgodnie ze standardem WCAG 2.1 oraz ustawą o dostępności stron internetowych i aplikacji mobilnych podmiotów publicznych z dnia 4 kwietnia 2019r.
Zawartość serwisu	Liczba i nazwy podstron do ustalenia
Usługi dodatkowe	• Konto pocztowe e-mail • Hosting WWW • Optymalizacja i pozycjonowanie • Pomoc techniczna • Mapa strony • Trzy wersje językowe

11. Audyt z cyberbezpieczeństwa zawierający:

- Audyt KRI
- Testy penetracyjne
- Audyt Bezpieczeństwa Informacji
- Audyt ciągłości działania
- Audyt zgodności z aktualnymi aktami prawnymi
- Audyt zgodności z RODO
- Audyt względem Krajowego System Cyberbezpieczeństwa

Dokumentacja poaudytowa wykonana w oparciu o regulacje prawne:

- Instrukcja Zarządzania Systemem Informatycznym,
- Polityka Bezpieczeństwa Danych Osobowych,
- Polityka Bezpieczeństwa Informacji,
- Polityka Bezpieczeństwa Tajemnic Przedsiębiorstwa,
- Polityka Bezpieczeństwa Informacji Poufnych lub Niejawnych.

Wykonawca zobowiązany będzie do:

- Wdrożenia zamówienia a w tym:
  - Przygotowanie procedur instalacji o Fizyczne wdrożenie sprzętu o Podłączenie elektryczne i sieciowe o Instalacja oprogramowania systemowego i zarządzającego o Testy poprawności działania systemów o Weryfikacja procesów przepływu danych i wydajności systemu o Serwis: Dostawa części Next Business Day + pomoc zdalna o Konsultacje techniczne w ramach umowy serwisu
- Wsparcie proaktywne a w tym:
  - cykliczna kontrola poprawności pracy systemów, zarządzanie poprawkami
- Wsparcie reaktywne a w tym:
  - wsparcie telefoniczne oraz konsultacje o Wsparcie w rozwoju system.