AG.271.1.1.2022

Załącznik Nr 2 do zapytania ofertowego

Szczegółowy Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest zakup sprzętu i oprogramowania w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00.

1. Ogólne warunki realizacji Zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie nw. elementów we wskazanych ilościach do siedziby Zamawiającego.
2. Zaoferowany przez Wykonawcę sprzęt i oprogramownie musi spełniać minimalne wymagania postawione w niniejszym załączniku.
3. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia nieograniczonej czasowo licencji Zamawiającemu.

2. Wymagania minimalne dla sprzętu i oprogramowania

2.1 Komputer stacjonarny – 10 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Typ	Komputer stacjonarny typu All in One
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych.
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych, TDP wynoszące min. 65W. Procesor osiągający w teście Passmark CPU Mark, wynik co najmniej 12300 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net w dniu 17.08.2022 r. Do oferty należy załączyć wydruk z ww. strony.
Pamięć RAM	8GB DDR4 2666MHz, jeden slot wolny. Możliwość rozbudowy do min 64GB
Pamięć masowa	Dysk M.2 SSD 256GB PCIe NVMe Obudowa musi umożliwić montaż dodatkowego dysku 2.5".
Karta graficzna	Zintegrowana z płytą główną
Matryca	Matryca FHD (1920 x 1080) w rozmiarze min. 23.8" IPS, z powłoką przeciwodblaskową (matowa), podświetlenie LED, jasność 250cd/m2, kontrast 1000:1, kąty widzenia matrycy 178 stopni poziomo oraz pionowo
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki o mocy min. 5W każdy. Wbudowany na bocznej krawędzi

	czytnik kart multimedialnych z obsługą min. formatu SD, SDHC,SDXC Wbudowana w obudowę matrycy cyfrowa kamera FHD (1920x1080). Wbudowany w obudowę mechanizm umożliwiający skuteczne zasłonięcie obiektywu kamery. Funkcjonalność realizowana na przykład poprzez wsunięcie kamery w górną krawędź obudowy. Dwa cyfrowe mikrofony
Obudowa	Typu All-in-One – płyta główna, procesor, dysk twardy oraz inne komponenty zintegrowane z monitorem min. 23,8" w jednej obudowie. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej. Blokada ma uniemożliwiać otwarcie obudowy. Montaż oraz demontaż podstawy nie może wymagać użycia narzędzi, a mocowanie podstawy musi posiadać przycisk zwalniający. Tylna pokrywa obudowy demontowana bez narzędziowo. Nie dopuszcza się stosowania śrub motylkowych, radełkowych, czy zwykłych wkrętów. Suma wymiarów samej obudowy (bez podstawy) nie może przekraczać 940mm. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, ponadto musi on być wpisany na stałe w BIOS. Zasilacz wewnętrzny o mocy max. 160W pracujący w sieci 230V 50/60Hz prądu zmiennego, cechujący się sprawnością na poziomie min. 85% przy 50% obciążeniu. Podstawa jednostki typu All – in – One musi umożliwiać: • Regulację wysokości w zakresie minimum 10 cm. • Obrót podstawy w lewą oraz prawą stronę. • Regulację pochyłu pionowego w zakresie od -5 do 30 stopni.
Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio, o zainstalowanej licencji systemu operacyjnego na płycie głównej. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.

	Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania, które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
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 wraz z możliwością wyświetlania danych SMART - test matrycy LCD - test magistrali PCI-e - test portów USB - test CPU - test myszy i klawiatury Wizualna sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: - Komputer: Producent, PN, model -BIOS: Wersja oraz data wydania Bios -Procesor: ilość rdzeni, wątków, obsługiwane instrukcje i pamięć cache -Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci -Dysk twardy: model, numer seryjny, wersja firmware, pojemność, prędkość obrotowa, temperatura pracy -LCD: producent, model, rozmiar, rozdzielczość
Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi i pakietami biurowymi.

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. 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, 5. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 7. Wbudowany system pomocy w języku polskim. 8. Możliwość dokonywania aktualizacji i poprawek systemu operacyjnego, 9. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 10. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 11. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 12. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 13. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 14. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 15. Wbudowany mechanizm wirtualizacji typu hypervisor. 16. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 17. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 18. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny. 19. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 20. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub

	klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 21. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 22. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 23. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 24. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 25. 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 26. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 27. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 28. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 29. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 30. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń 31. Klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. 32. Współpraca systemu z usługami domenowymi Active Directory
Certyfikaty i standardy	Deklaracja zgodności CE Energy Star EPEAT Urządzenia wyprodukowane zgodnie z normą ISO9001 Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki

Wymagania dodatkowe	Wbudowane porty: • 1 x DisplayPort++ 1.4a/HDCP 2.3 port • 1 x HDMI In 1.4 • 1 x HDMI Out 2.0 • 1x USB 3.2 Gen 2 Type-C • 1x USB 3.2 Gen 1 • 4 x USB 3.2 Gen 2 • 1 x port audio typu combo (słuchawka/mikrofon) • 1 x RJ – 45 (10,100,1000 Mbit/s), karta zintegrowana z płytą główną -Gniazdo karty SD -Karta WLAN 2x2 802.11ax z Bluetooth w wersji nie niższej niż 5 -Złącze typu Kensington Lock Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w: min. 2 złącza SO DIMM z obsługą do 64GB DDR4 pamięci RAM, min. Przynajmniej jedno złącze z obsługą protokołu SATA III umożliwiające bezpośrednie podłączenie oraz zasilanie dodatkowego dysku (bez stosowania kabli zasilających). Dwa złącza M.2 dla dysków. Bezprzewodowa mysz oraz bezprzewodowa klawiatura w układzie polski programisty. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
Warunki gwarancji	5-letnia gwarancja producenta świadczona na miejscu u klienta, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną producenta. W przypadku awarii, dyski twarde zostają u Zamawiającego. Czas reakcji serwisu - do końca następnego dnia roboczego. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie producenta komputera.
Dodatkowe oprogramowanie	Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne

2.2. Oprogramowanie biurowe – 10 szt.

Nazwa	Opis minimalnych parametrów
Oprogramowanie biurowe	Pakiet biurowy (wraz z licencją na czas nieokreślony, kluczem instalacyjnym tego oprogramowania): Microsoft Office 2019 PL lub innego oprogramowania biurowego równoważnego, zawierającego co najmniej: edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej oraz kalendarza, które charakteryzuje się następującymi cechami: - całkowicie zlokalizowany w języku polskim interfejs, system komunikatów i podręcznej kontekstowej pomocy technicznej (w tym także on-line) w pakiecie, - możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego), - możliwość zdalnej instalacji komponentów, - możliwość prowadzenia dyskusji oraz subskrypcji dokumentów w sieci z automatycznym powiadomieniem o zmianach w dokumentach, oraz publikowanie dokumentów wprost z komponentów pakietu np. arkusza kalkulacyjnego, - w systemach pocztowych - możliwość delegacji uprawnień do otwierania, drukowania, modyfikowania i czytania załączanych dokumentów i informacji, - możliwość blokowania niebezpiecznej lub niechcianej poczty, - automatyczne przesyłanie poczty na podstawie reguł, automatyczne odpowiedzi, potwierdzanie dostarczenia do skrzynki adresata oraz potwierdzanie otwarcia poczty u adresata, - współpraca z systemem MS Exchange, w tym odbiór poczty, możliwość udostępniania kalendarza dla innych użytkowników, - wsparcie dla formatu XML w podstawowych aplikacjach, - możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich fragmentów, - automatyczne wyróżnianie i aktywowanie hyperlinków w dokumentach podczas edycji i odczytu, - możliwość automatycznego odświeżania danych pochodzących z Internetu w arkuszach kalkulacyjnych, - możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony, - możliwość zaszyfrowania danych w dokumentach i arkuszach kalkulacyjnych zgodnie ze standardem CryptoAPI, - możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych w wypadku odcięcia dopływu prądu, - prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach:.doc, .docx, xls,.xlsx, ppt, .pptx, .pps, .ppsx, w tym obsługa formatowania, wykonywanie i edycję makr oraz kodu zapisanego w języku Visual Basic for Application w plikach xls, xlsx, formuł, formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010 bez utraty danych oraz bez konieczności reformatowania dokumentów, - prawidłowe otwieranie i zapisywanie plików o formatach doc, docx, xls, xlsx, .ppt, pptx. .pps, .ppsx bez utraty parametrów i cech użytkowych zachowane wszelkie formatowanie, umiejscowienie tekstów, liczb, obrazków, wykresów, odstępy między tymi obiektami i kolorów, działające makra,

	- prawidłowa współpraca zapis, odczyt z plikami danych programów pocztowych w formacie .pst oraz prawidłowy import z formatu .dbx, - wszystkie komponenty oferowanego pakietu biurowego (edytor, arkusz, klient poczty, kalendarz oraz program do prezentacji) muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi, poprawna praca w systemach operacyjnych w które może być wyposażony zamawiany zestaw, tj. 64-bitowych z rodziny Windows 7, Windows 8, Windows 8.1, Windows 11, - w przypadku zaoferowanego oprogramowania równoważnego należy podać dokładną nazwę i wersję oferowanego produktu, - zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.

2.3. Urządzenie zapory sieciowej typu UTM z wdrożeniem – 1 szt.

Parametr	Opis wymagań minimalnych
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	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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN.
Interfejsy, Dysk, Zasilanie:	System realizujący funkcję Firewall musi dysponować minimum: 8 portami Gigabit Ethernet RJ-45, 2 portami WAN (RJ45), 2 portami SFP 1 Gbps. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:	W zakresie Firewall'a obsługa nie mniej niż 1,4 mln równoczesnych sesji oraz 45 tys. nowych połączeń na sekundę. Przepustowość Firewall: nie mniej niż 10 Gbps dla pakietów 1518 (bajtowe pakiety UDP) Przepustowość Firewall: nie mniej niż 7 Gbps dla pakietów 64 (bajtowe pakiety UDP) Przepustowość Firewall: nie mniej niż 10 Gbps dla pakietów 512 (bajtowe pakiety UDP) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,7 Gbps. Wydajność szyfrowania IPSec VPN (512 bajtów) nie mniej niż 6 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) - min. 1.4 Gbps Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Kontrola Aplikacji, Antywirus - minimum 900 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 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. 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	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 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. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 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	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. 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	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	System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 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. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 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. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 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	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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie	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. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: - 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	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.

Wdrożenie (wsparcie techniczne)	System musi być objęty wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu, w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Partnera Serwisowego Producenta świadczona w języku polskim w zakresie: - wsparcie telefoniczne zespołu certyfikowanych inżynierów - pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu - doradztwo w zakresie konfiguracji - zdalne wsparcie techniczne (w trybie 8x5) - pomoc w zakładaniu zgłoszeń serwisowych u producenta - pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta - przygotowanie urządzenia do zdalnej konfiguracji - zdalna konfiguracja urządzenia zgodnie z wymaganiami użytkownika - rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań klienta - usługa upoważnia do maksymalnie 10 zdalnych zmian w konfiguracji Dostęp do usługi świadczony przez dedykowaną infolinię oraz przez dedykowany moduł internetowy. Usługa ta ma być świadczona prze podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Wykonawca dostarczy oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

2.4. Zakup oprogramowania do tworzenia kopii zapasowych i archiwizacji danych z wdrożeniem – 1 szt.

Nazwa	Opis wymagań minimalnych
Oprogramowanie	Zakup aktualizacji posiadanego przez Zamawiającego oprogramowania Ferro Backup System 5 Standard do najnowszej wersji 6. Wraz z dostarczeniem licencji Zamawiający wymaga wsparcia technicznego polegającego na dostosowaniu obecnej instalacji Ferro Backup System na urządzeniu Synology NAS do nowej wersji programu obejmującą: - aktualizacja ma dotyczyć oprogramowania systemowego urządzenia, pakietów oprogramowania służącego integracji oraz komponentów programowych systemu zarówno na serwerze jak i na końcówkach klienckich z zachowaniem wskazanych danych oraz ustawień, - pełne zdalne dostosowanie systemu do wymagań najnowszej wersji Ferro Backup System - konfiguracja systemu wraz z zachowaniem wszystkich kopii bezpieczeństwa i ciągłości wykonywania kopii danych - aktualizacja systemu DSM urządzenia Synology do najnowszej wersji - weryfikacja poprawności wykonywanych backupów - weryfikacja konfiguracji zadań backupu - przegląd poziomu realizacji zadań backupu i pomoc w usunięciu ewentualnych nieprawidłowości - sprawdzenie ogólnej kondycji sprzętu na podstawie dziennika zdarzeń raportowanych przez system

	- Wykonawca dostarczy referencje świadczące o równoważnych wdrożeniach systemów do wykonywania backup - wsparcie techniczne 12 miesięcy na wdrożone rozwiązanie