Załącznik Nr 4 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Specyfikacja techniczna / funkcjonalna przedmiotu zamówienia

Niniejszy dokument określa minimalne wymagania dla przedmiotu zamówienia dotyczącego postępowania o udzielenie zamówienia publicznego pn.: **Dostawa infrastruktury sprzętowej i oprogramowania, wykonanie diagnozy cyberbezpieczeństwa, a także przeprowadzenie szkoleń w ramach realizacji przez Gminę Brzeźnica projektu „Cyfrowa Gmina”.**
Zakup jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego 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, dotyczący realizacji projektu grantowego „Cyfrowa Gmina” dla Gminy Brzeźnica o numerze POPC.05.01.00-00-0001/21-00.

WYMAGANIA MINIMALNE

1. Serwer

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne – opcjonalnie możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane dwa procesory 8-rdzeniowy, min. 2,8 GHz, klasy ×86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 127 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	128 GB DDR4 RDIMM 3200 MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1 TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing.
Gniazda PCI	Minimum dwa słoty PCIe ×16 generacji 4.
Interfejsy sieciowe/ FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1 Gb Ethernet w standardzie BaseT.
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD. Zainstalowane 4 dyski SSD SATA MixUse o pojemności min. 480 GB, 6 Gb, 2,5" Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480 GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64 GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 4 GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
System operacyjny/dodatkowe oprogramowanie	Zamawiający wymaga, aby dostarczony serwer posiadał zainstalowane oprogramowanie systemowe w najnowszej aktualnej wersji, nieograniczonej czasowo wraz z licencją dostępową dla 25 użytkowników. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w środowisku fizycznym

	i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Poniższy opis należy traktować jako zbiór wymagań minimalnych, ponieważ Wykonawca musi zapewnić odpowiednie parametry i spełnić wszystkie wymagania licencyjne oferowanego systemu operacyjnego, niezbędne do poprawnego uruchomienia rozwiązania. SSO musi posiadać następujące, wbudowane cechy: ✓ możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, ✓ możliwość wykorzystywania 64 procesorów wirtualnych oraz 1 TB pamięci RAM i dysku o pojemności min. 64 TB przez każdy wirtualny serwerowy system operacyjny, ✓ możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8 000 maszyn wirtualnych, ✓ 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, ✓ wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, ✓ wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, ✓ automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, ✓ możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), ✓ wbudowane wsparcie instalacji i pracy na wolumenach, które: • pozwalają na zmianę rozmiaru w czasie pracy systemu, • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, • umożliwiają zdefiniowanie list kontroli dostępu (ACL), ✓ wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, ✓ wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 ✓ możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, ✓ możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, ✓ wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, ✓ graficzny interfejs użytkownika, ✓ zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, ✓ wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), ✓ możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, ✓ dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, ✓ możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: • podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, • 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: – podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, – ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, – odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, • zdalna dystrybucja oprogramowania na stacje robocze, • praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: – dystrybucję certyfikatów poprzez http, – konsolidację CA dla wielu lasów domeny, – automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, • szyfrowanie plików i folderów, • szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), • możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, serwis udostępniania stron WWW, • wsparcie dla protokołu IP w wersji 6 (1Pv6), wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 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: – dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, – obsługi ramek typu jumbo frames dla maszyn wirtualnych, obsługi 4-KB sektorów dysków, – nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, – możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, – możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), • możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, • wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), • możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, • mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, ✓ możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WSManagement organizacji DMTF.
Wbudowane porty	Przednie: min. 1 × VGA, min. 1 × USB 2.0, min. 1 × micro-USB dedykowane dla karty zarządzającej. Tylne: min. 1 × VGA, min. 2 × USB w tym 1 × USB 3.0.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600 × 900.
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 800 W.
Bezpieczeństwo	✓ zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych, ✓ możliwość wyłączenia w BIOS funkcji przycisku zasilania, ✓ BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła,

	✓ wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą, ✓ moduł TPM 2.0, ✓ możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera, ✓ możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ✓ zdalny dostęp do graficznego interfejsu Web karty zarządzającej, ✓ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera), ✓ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, ✓ możliwość podmontowania zdalnych wirtualnych napędów, ✓ wirtualną konsolę z dostępem do myszy, klawiatury, ✓ wsparcie dla IPv6, ✓ wsparcie dla WSMAN (Web Service for Management), SNMP, IPMI 2,0, SSH, Redfish, ✓ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, ✓ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ✓ integracja z Active Directory, ✓ możliwość obsługi przez dwóch administratorów jednocześnie, ✓ wsparcie dla dynamic DNS, ✓ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, ✓ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera, ✓ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
Certyfikaty/normy	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Warunki gwarancji	3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24 × 7 × 365 poprzez ogólnopolską linię telefoniczną producenta. Naprawa realizowana w miejscu instalacji. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Ilość	1 szt.

2. UPS

Nazwa	Minimalne wymagania dla sprzętu	
Typ	Zasilacz awaryjny UPS	
Wymagania techniczne	Moc pozorna	minimum 3000 VA
	Moc rzeczywista	minimum 2250 W
	Topologia	VI (line interactive)
	Typ obudowy	rack; z możliwością instalacji jako tower. Wymagane wsporniki do montażu w szafir RACK
	Chłodzenie	Wymuszone, wewnętrzne wentylatory
	Wejście	
	Napięcie znamionowe (wartość skuteczna)	230 V AC
	Zakres napięcia wejściowego (wartości skuteczne) i tolerancja	178 + 281 V AC ±
	Częstotliwość znamionowa napięcia wejściowego	50 Hz
	Zakres częstotliwości i tolerancja	45 + 55 1
	Progi przełączania: sieć – UPS	178 + 281 V AC ± 2 %
	Wyjście	
	Napięcie znamionowe (wartość skuteczna)	230 V AC
	Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa	195 + 253 V AC ±
	Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja — praca rezerwowa	230 V AC ±
	Automatyczna regulacja napięcia (AVR)	± 10 %
	Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej)	Sinusoidalny / Tak jak na wejściu
	Częstotliwość znamionowa napięcia wyjściowego	50 Hz
	Filtracja napięcia wyjściowego	Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy
	Progi przełączania: UPS — sieć	183 + 276 V AC ± 2 %
	Czas przełączenia na pracę rezerwową	< 3 ms
	Czas powrotu na pracę sieciową	0 ms
	Przeciążalność	> 105% - 15 s (wyłączenie UPS)
	Akumulatory i czasy podtrzymania	
	Akumulatory wewnętrzne	minimum 12 V / 9 Ah VRLA
	Czas podtrzymania z baterii wewnętrznych dla obciążenia 2250W	minimum 3 min
	Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii – po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza).	do 4 h
	Zabezpieczenia	
	Zabezpieczenie wejściowe	Przeciwzwarciowe – Bezpiecznik automatyczny 16 A/ 250 VAC Przeciwprzepięciowe

	Zabezpieczenie wyjściowe	Elektroniczne – przeciwzwarciowe i przeciążeniowe
	Zabezpieczenia wejścia DC (akumulatory wewnętrzne)	Zabezpieczenie nadprądowe
	Wyposażenie i funkcje dodatkowe	
	Przyłącza wyjściowe (liczba i typ gniazd)	minimum 8 gniazd z podtrzymaniem bateryjnym (w tym minimum 2 gniazda w standardzie PL z bolcem uziemiającym)
	Sygnalizacja	Akustyczno – optyczna; graficzny wyświetlacz LCD w języku polskim
	Interfejsy komunikacyjne	USB HID, SNMP/HTTP
	Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie napięcia sieciowego	wymagane
	Możliwość aktualizacji oprogramowania firmware przez użytkownika	wymagane
Gwarancja	minimum 36 miesiące na elektronikę i 24 miesiące na akumulatory.	
Serwis	Autoryzowany serwis producenta zlokalizowany w Polsce. Wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. Naprawa w maksymalnie 5 dni roboczych, Serwis realizowany w systemie door to door.	
Oprogramowanie	Oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS. Wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. Wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer. Oprogramowanie pozwala na w zakresie minimalnym: ✓ możliwość zdalnego włączenia / wyłączenia UPSa, ✓ możliwość edycji nazw urządzeń na liście monitorowanych UPSów.	
Certyfikaty producenta	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; deklaracja CE producenta sprzętu	
Oświadczenia / dokumenty	Oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji. Karta katalogowa oferowanego sprzętu	
Ilość	1 szt.	

3. Diagnostyka cyberbezpieczeństwa

Nazwa	Minimalne wymagania dla usługi
Typ	Wykonanie audytu diagnozy cyberbezpieczeństwa, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do dokumentacji konkursowej – Cyfrowa Gmina. Diagnoza cyberbezpieczeństwa powinna zostać przeprowadzona w terminie do 4 miesięcy od podpisania umowy. Wynikiem przeprowadzenia diagnozy musi być raport dotyczący audytowanego środowiska oraz wypełnienie formularza diagnozy i dostarczenia go za pomocą elektronicznej skrzynki podawczej ePUAP do NASK na adres skrzynki: /NASK-Instytut/SkrzynkaESP.
Plan audytu	Przeprowadzony audyt musi obejmować: ✓ audyt dokumentacji i procesów (Ocena zgodności z Krajowymi Ramami Interoperacyjności / Krajowym Systemie Cyberbezpieczeństwa, Ocena aspektów bezpieczeństwa systemów informatycznych, Ocena dojrzałości wybranych procesów bezpieczeństwa, Opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny), ✓ testy penetracyjne infrastruktury sieciowej (Przedstawienie założeń, weryfikacja

	dokumentacji sieci, topologii sieci, kluczowych elementów sieci, Skanowanie sieci, Skanowanie najistotniejszych hostów w sieci wybranych na podstawie wcześniejszej analizy, Sprawdzanie domyślnych haseł, Sprawdzanie możliwości wylistowania użytkowników oraz zdobycia haseł, Weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych, Weryfikacja zabezpieczeń urządzeń sieciowych, Testy socjotechniczne, Wykonanie raportu, Wsparcie poaudytowe).
Wymagania dla audytora	Audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu: ✓ Certified Information System Auditor (CISA), ✓ certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób, ✓ Certified Information Security Manager (CISM), ✓ Certified Information Systems Security Professional (CISSP).

4. Urządzenie klasy UTM

Nazwa	Minimalne wymagania dla urządzenia
Typ	Urządzenie klasy UTM wraz z niezbędnymi serwisami i aktualizacjami
Wymagania techniczne	Dostarczone urządzenie klasy UTM musi posiadać następujące minimalne funkcje: 1. OBSŁUGA SIECI w zakresie minimum: ✓ urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. 2. ZAPORA KORPORACYJNA (Firewall) w zakresie minimum: ✓ urządzenie ma być wyposażone w Firewall klasy Stateful Inspection, ✓ urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT, ✓ urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge), ✓ Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie, ✓ administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall, ✓ edytor reguł firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów), ✓ Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). 3. INTRUSION PREVENTION SYSTEM (IPS) w zakresie minimum: ✓ system detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe, ✓ moduł IPS musi być opracowany przez producenta urządzenia. Nie

	dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy, ✓ moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń, ✓ administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS, ✓ moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej, ✓ urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTFPS, FTPS, POP3S oraz SMTPS, ✓ administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP, ✓ urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0, ✓ urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie, ✓ moduł skanujący musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci, ✓ moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu. 4. KSZTAŁTOWANIE PASMA (Traffic Shapping) w zakresie minimum: ✓ urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma, ✓ ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP, ✓ rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring), ✓ urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. 5. OCHRONA ANTYWIRUSOWA w zakresie minimum: ✓ rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania, ✓ co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji, ✓ urządzenie ma być dostarczone wraz z komercyjnym skanerem antywirusowym, nie dopuszcza się stosowania skanera rozwijanego w ramach projektów OpenSource, ✓ administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym, ✓ administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. 6. OCHRONA ANTYSPAM w zakresie minimum ✓ producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM), ✓ ochrona antyspam ma działać w oparciu o: • białe/czarne listy, • DNS RBL, • heurystyczny skaner, ✓ w przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL, ✓ wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

	7. WIRTUALNE SIECI PRYWANTE (VPN) w zakresie minimum: ✓ urządzenie ma posiadać wbudowany filtr URL, ✓ filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych, ✓ administrator musi mieć możliwość dodawania własnych kategorii URL, ✓ urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. ✓ moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST, ✓ administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: • blokowanie dostępu do adresu URL, • zezwolenie na dostęp do adresu URL, • blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora, ✓ administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony, ✓ strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych, ✓ filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS, ✓ urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME, ✓ urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 8. FILTR DOSTĘPU DO STRON WWW w zakresie minimum: ✓ urządzenie ma posiadać wbudowany filtr URL, ✓ filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 65 kategorii tematycznych stron internetowy, ✓ w ramach filtra URL sklasyfikowanych jest co najmniej 100 milionów stron internetowych, ✓ administrator musi mieć możliwość dodawania własnych kategorii URL, ✓ urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora, ✓ moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST, ✓ administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: • blokowanie dostępu do adresu URL, • zezwolenie na dostęp do adresu URL, • blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora, ✓ administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony, ✓ strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych, ✓ filtrowanie URL musi uwzględniać także komunikację po protokole, ✓ urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME, ✓ urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 9. UWIERZYFELNIANIE w zakresie minimum: ✓ urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: • lokalną bazę użytkowników (wewnętrzny LDAP), • zewnętrzną bazę użytkowników (zewnętrzny LDAP), • usługę katalogową Microsoft Active Directory ✓ rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP, ✓ rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:

	• SSL, • Radius, • Kerberos. ✓ urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory, ✓ co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta, ✓ autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. 10. ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP) w zakresie minimum: ✓ urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing), ✓ mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: • równoważenie względem adresu źródłowego, • równoważenie względem połączenia, ✓ mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu, ✓ urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego, ✓ urządzenie ma posiadać mechanizm statycznego trasowania pakietów, ✓ urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego, ✓ urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP, ✓ rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 11. POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA w zakresie minimum: ✓ urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci, ✓ urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay, ✓ konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i 1Pv6, ✓ urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS, ✓ urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1, 2 i 3, ✓ urządzenie musi posiadać usługę DNS Proxy. 12. ADMINISTRACJA URZĄDZENIEM w zakresie minimum: ✓ konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego, ✓ interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https, ✓ komunikacja może odbywać się na porcie innym niż https (443 TCP), ✓ urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami, ✓ rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana, ✓ interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https, ✓ urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). ✓ rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. ✓ urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej

	ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora, ✓ urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury/ producenta lub z dedykowanego urządzenie musi posiadać funkcjonalność anonimizacji logów, ✓ urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów. ✓ wraz z urządzeniem musi zostać dostarczona kompatybilna z urządzeniem klasy UTM, karta pamięci typu SD o pojemności minimum 128 GB, o klasie prędkości minimum 10. 13. RAPORTOWANIE w zakresie minimum: ✓ urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania, ✓ system raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego, ✓ system raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów, ✓ system raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu, ✓ w ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny, ✓ dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy. 14. PARAMETRY SPRZĘTOWE w zakresie minimum: ✓ urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash, ✓ liczba portów Ethernet 10/100/1000Mbps – min. 8, ✓ urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta, ✓ przepustowość Firewall — min. 4 Gbps. ✓ przepustowość Firewall wraz z włączonym systemem IPS – min. 2,4 Gbps, ✓ przepustowość filtrowania Antywirusowego – min. 495 Mbps, ✓ minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps, ✓ maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100, maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20, ✓ obsługa min. VLAN 64, ✓ liczba równoczesnych sesji – min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę. ✓ urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. Urządzenie jest nielimitowane na użytkowników.
Gwarancja	Wymaga się, aby dostawa obejmowała również minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu oraz licencje dla wszystkich funkcji bezpieczeństwa.
Ilość	1 szt.

5. Oprogramowanie do monitorowania sieci

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do monitorowania sieci. Licencja powinna pozwalać na użytkowanie oprogramowania przez min. 120 użytkowników. Oprogramowanie musi posiadać następujące minimalne funkcjonalności.
Monitorowanie infrastruktury	Oprogramowanie musi umożliwiać minimum: Wykrywanie urządzeń w sieci poprzez skanowanie ping (oraz arp-ping). Wizualizacja stanu urządzeń w postaci ikon urządzeń na mapach sieci.

	Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Program powinien monitorować czas ich odpowiedzi i procent utraconych pakietów. Serwerów pocztowych: ✓ program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę, ✓ program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS), w razie, gdyby przestały one odpowiadać lub funkcjonowały wadliwie, ✓ program powinien mieć możliwość wykonywania operacji testowych, ✓ program powinien mieć możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa. Monitorowanie serwerów WWW i adresów URL. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 (przełączniki, routery, drukarki sieciowe, urządzenia VoIP). Obsługa komunikatów syslog i pułapek SNMP. Monitoring routerów i przełączników wg: ✓ zmian stanu interfejsów sieciowych, ✓ ruchu sieciowego, ✓ podłączonych stacji roboczych, ✓ ruchu generowanego przez podłączone stacje robocze. Wydajności systemów z rodziny Windows posiadanych przez Zamawiającego: ✓ obciążenie CPU pamięci, zajętość dysków transfer sieciowy.
Gromadzenie informacji o sprzęcie i oprogramowaniu	Oprogramowanie musi umożliwiać minimum: Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. Informacja o zainstalowanych aplikacjach oraz aktualizacjach co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. Zbieranie informacji w zakresie zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP. Posiadanie możliwości wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. Możliwość odczytania numeru seryjnego (klucze licencyjne). Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. Możliwość przeglądu informacji o konfiguracji systemu, tj. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników harmonogramie zadań.
Zdalna pomoc dla użytkowników	Oprogramowanie musi umożliwiać minimum: W ramach kontroli stacji użytkownika dostępny powinien być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. Pobieranie listy użytkowników z usługi katalogowej. Przypisywanie pracowników helpdesk do kategorii zgłoszeń. Procesowanie zgłoszeń użytkowników z wiadomości e-mail. Dołączanie załączników do zgłoszeń. Zrzuty ekranowe (podgląd pulpitu). Dystrybucję oprogramowania przez Agentów. Dystrybucję oraz uruchamianie plików za pomocą Agentów. Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku. Możliwość skonfigurowania automatyzacji procesowania zgłoszeń.

	Planowanie nieobecności pracowników helpdesk. Obsługę umów o gwarantowanym poziomie świadczenia usług (SLA). Generowanie raportów obsługi helpdesk. Zdalne wykonywanie poleceń poprzez Agentów (utworzenie /edycja konta lokalnego użytkownika systemu). Możliwość użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Oprogramowanie powinno posiadać komunikator. Oprogramowanie powinno posiadać bazę zgłoszeń umożliwiającą użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.
Aktywność użytkowników	Oprogramowanie musi umożliwiać minimum: Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach. Monitorowanie rzeczywistego użytkowania programów (procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt). Monitorowania transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika). Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen. Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Wyświetlanie statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. Wyświetlanie statystyki aktywności grupy i jej członków widoczne dla menedżera grupy. Grupowanie stron internetowych oraz aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). Przypisywanie kategorii aplikacjom i stronom internetowym, możliwość stworzenia predefiniowanej listy kategorii z możliwością edycji. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji.
Ochrona danych przed wyciekiem	Oprogramowanie musi umożliwiać minimum: Zarządzanie prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.

	Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. Autoryzowanie urządzeń firmowych: pendrive'ów, dysków zewnętrznych – urządzenia nieautoryzowane. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Możliwość usuwania z listy znanych urządzeń tych nośników.
Warunki licencji	Licencja na użytkowanie oprogramowania musi być wieczysta. Musi dawać możliwość wsparcia oraz aktualizacji przez okres 1 roku. Licencja musi pozwalać na użytkowanie oprogramowania przez minimum 35 użytkowników

6. Urządzenie do backupu

Nazwa	Minimalne wymagania dla sprzętu
Typ	Urządzenie typu NAS
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3,5 calowych SATA 6 Gb/s, 3Gb/s, wraz z kompletem szyn umożliwiających montaż w szafie rack. Na urządzeniu znajdują się wskaźniki LED informujące min o HDD 1-8, stan, LAN, rozszerzenie, zasilanie
Procesor	Zainstalowany jeden procesor 4-rdzeniowy, min. 2.0GHz, 64 bitowy x86, klasy serwerowej.
Pamięć RAM	Zainstalowane min. 4 GB SO-DIMM DDR4 (1 × 4 GB), możliwość rozszerzenia pamięci RAM min. do 16 GB.
Gniazda PCI	Min. 1 × PCIe Gen3 × 2.
Interfejsy sieciowe	2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M) obsługa VLAN i Jumbo Frame.
Dyski twarde	Zamontowane 4 dyski 3,5-cala HDD, min. 4 TB SATA, 7200RPM, 256 MB cache, min. 2 mln MTBF, przeznaczone do pracy 24/7, serii Enterprise, gwarancja producenta 60 miesięcy.
Porty USB	Urządzenie posiada min. 2 × USB 2.0, 2 × USB 3.2 Gen 2, 1 × HDMI 1.4b.
Wspierane Systemy Operacyjne	Apple Mac OS 10.10 i późniejsze Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 i późniejsze Linux IBM AIX 7, Solaris 10 lub późniejsze UNIX Microsoft Windows 7, 8, i 10 Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,55+Spare,6,6+Spare10 i 10+Spare, RAID50, RAID60. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk. Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem min. AES 256 bitów.
Wentylatory	Minimum 2 każdy po 8 cm.
Zasilanie	Redundantne, min.2x 300W. Urządzenie posiada możliwość obsługi sieciowych awaryjnych zasilaczy UPS.
Stacja monitoringu	Obsługa do 24 kamer IP (8 licencji domyślnie).
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iscsł, Telnet, SSH, SNMP
Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Virtualization Station.
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski.
Gwarancja	Gwarancja minimum 36 miesięcy na NAS. Gwarancja minimum 60 miesięcy na dyski.
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+.
iSCSl	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation.
Liczba kont użytkownika	min. 4096.

Liczba grup	512.
Liczba udziałów	512.
Minimalna ilość połączeń	1500.
Minimalna liczba migawek	1024.
Zasilanie	Redundantne 300 W (×2), 100-240 V.
Wentylatory	2 × 80 mm, 12 VDC.
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.

7. Szkolenie dla pracowników z zakresu cyberbezpieczeństwa

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenie zdalne dla pracowników Urzędu z zakresu cyberbezpieczeństwa
Program szkolenia	1. Czym jest cyberbezpieczeństwo? 2. Podstawowe przedstawienie zagadnienia cyberbezpieczenstwa. 3. Przedstawienie zagrożeń, które czyhają na nas w sieci (rodzaje zagrożeń i ich konsekwencje. 4. Opis i wymagania normy ISO/IEC 27001. 5. Dlaczego wiedza o cyberbezpieczeństwie jest konieczna? 6. Sposoby ochrony kont i danych przed potencjalnym zagrożeniem. 7. Częsta zmiana haseł, czy ustalanie ich odpowiedniej trudności a co za tym idzie programy pomagające w tym (np. keypas) 8. Logowanie w sieci. 9. Opis Certyfikatów stron internetowych. 10. Darmowe WiFi i automatyczne podłączanie się. 11. Praca zdalna – czym jest VPN i jak z niego korzystać? 12. Wprowadzenie do sieci komputerowych – niebezpieczeństwo sieci otwartych bezprzewodowych. 13. Niezabezpieczone protokoły sieciowe – HTFP FTP. 14. Zaszyfrowana komunikacja w Internecie (Signal i WhatsApp). 15. Ochrona plików i dysków czyli podstawy szyfrowania. 16. Przedstawienie przykładów i nauka rozpoznawania niepożądanych maili i ich zawartości. 17. Odpowiednia weryfikacja odbiorcy i nadawcy. 18. Weryfikacją wiadomości e-mail. 19. Weryfikacja i skan plików znajdujących się w załączniku. 20. Przykłady ataków oraz sposoby na ochronę przed nimi pod kątem zwykłego użytkownika. 21. Phishing i td – sposoby na zabezpieczenie się przed włamaniami i oszustwem w sieci. 22. Programy antywirusowe i ich rola (omówienie popularnych programów i opis ich działania). 23. Tworzenie kopii zapasowych i ich odzyskiwanie po awarii. 24. Sposoby tworzenia backup'ów. 25. Podpis elektroniczny dokumentów w prosty i bezpieczny sposób.
Wymagania dodatkowe	W ramach realizacji szkolenia wymagane jest, aby: ✓ szczegółowy harmonogram szkolenia został uzgodniony z Zamawiającym terminie minimum 14 dni przed terminem rozpoczęcia szkolenia, ✓ szkolenie zostanie przeprowadzone w maksymalnie 2 turach po 4 godziny, ✓ uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych, ✓ uczestnik po zakończeniu szkolenia musi otrzymać zaświadczenie ukończenia szkolenia, ✓ uczestnik musi mieć możliwość bezpłatnego 14-sto dniowego kontaktu z trenerem po szkoleniu.
Ilość	35 pracowników.

WYMAGANIA DODATKOWE

W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do dostawy przedmiotu zamówienia wraz z jego rozpakowaniem, sprawdzeniem poprawności działania i ustawieniem w wyznaczonym przez Zamawiającego pomieszczeniu na terenie Urzędu.
Wykonawca zobowiązany do utylizacji na własny koszt wszelkich niepotrzebnych materiałów zabezpieczających urządzenia podczas transportu, w tym kartony, folie, taśmy klejące etc.
Wykonawca zobowiązany jest do ustalenia terminów dostaw z Zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Urzędu.