sfinansowano w ramach reakcji Unii na pandemię COVID-19

ZAŁĄCZNIK NR 1 DO SWZ

Opis Przedmiotu Zamówienia

Infrastruktura sprzętowa i oprogramowanie,
audyt cyberbezpieczeństwa,
szkolenie z zakresu cyberbezpieczeństwa

sfinansowano w ramach reakcji Unii na pandemię COVID-19

Specyfikacja techniczna / funkcjonalna przedmiotu zamówienia

Spis treści

Wstęp

Niniejszy dokument określa minimalne wymagania dla dostawy infrastruktury sprzętowej i oprogramowania, wykonania: diagnozy cyberbezpieczeństwa (audytu) a także przeprowadzenia szkolenia dla pracowników Urzędu Gminy Wiejskiej Gubin z zakresu cyberbezpieczeństwa w ramach realizacji projektu pn.: „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 Gubin o statusie wiejskim o numerze 0802025

sfinansowano w ramach reakcji Unii na pandemię COVID-19

1. Modernizacja posiadanego sprzętu serwerowego – 1 kpl.

Lp.	Nazwa komponentu	Wymagane minimalne parametry
1	2	3
Modernizacja posiadanego sprzętu serwerowego		
1.	**Dysk SSD - serwer**	Zamawiający wymaga dostarczenia min. 2 szt. dysków min. 480 GB SSD do aktualnie posiadanego serwera Dell PowerEdge R440 o numerze seryjnym: HF5XJ23.
2.	**Pamięć RAM - serwer**	Zamawiający wymaga dostarczenia min. 2 szt. kości RAM min. 32GB do aktualnie posiadanego serwera Dell PowerEdge R440 o numerze seryjnym: HF5XJ23.

2. Serwer z oprogramowaniem systemowym – 1 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry
1	2	3
Serwer z oprogramowaniem systemowym		
1.	**Obudowa**	Obudowa Rack o wysokości max 1U z możliwością instalacji minimum 4 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
2.	**Płyta główna**	Płyta główna z możliwością zainstalowania do dwóch procesorów.
3.	**Chipset**	Dedykowany do pracy w serwerach dwuprocesorowych
4.	**Procesor**	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.8 GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 125 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
5.	**RAM**	Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
6.	**Funkcjonalność pamięci RAM**	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
7.	**Gniazda PCI**	- minimum dwa sloty PCIe x16 generacji 4
8.	**Interfejsy sieciowe/FC/SAS**	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
9.	**Dyski twarde**	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane minimum 2 dyski SSD SATA o pojemności min. 960GB, Hot-Plug. Możliwość zainstalowania min. dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
10.	**Kontroler RAID**	Sprzętowy kontroler dyskowy posiadający min. 4GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
11.	**System operacyjny/dodatkowe oprogramowanie**	Zamawiający wymaga, aby dostarczony serwer posiadał zainstalowane oprogramowanie systemowe w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać min. do uruchamiania oprogramowania systemowego (dalej: SSO) w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Wykonawca odpowiada za sprawne i wydajne działanie systemu operacyjnego na dostarczonym sprzęcie serwerowym. 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 min. następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych, d) 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, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),

		s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. 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: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. 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: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

		2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) 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, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
12.	**Wbudowane porty**	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
13.	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
14.	**Wentylatory**	Redundantne
15.	**Zasilacze**	Redundantne, Hot-Plug maksymalnie 800W.
16.	**Bezpieczeństwo**	● 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
17.	**Diagnostyka**	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
18.	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca min.: ● zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ● zdalne monitorowanie i informowanie o statusie serwera (min. 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; IPMI2.0, 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
19.	**Certyfikaty**	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE.
20.	**Warunki gwarancji**	Minimum 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną producenta. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. W przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem - dokument potwierdzający załączyć do formularza ofertowego Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
21	**Dokumentacja użytkownika**	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

3. Stacja robocza z systemem operacyjnym – 14 kpl.

Lp.	Nazwa komponentu	Wymagane minimalne parametry urządzenia
1	2	3
Stacja robocza z systemem operacyjnym		
1.	**Typ**	Komputer stacjonarny.
2.	**Zastosowanie**	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych.
3.	**Wydajność obliczeniowa**	Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 12 400 punktów według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php
4.	**Pamięć RAM**	Minimum 8GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB. Jeden slot DIMM wolny.
5.	**Pamięć masowa**	Dysk M.2 SSD Minimum 256GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”
6.	**Wydajność grafiki**	Zintegrowana z procesorem
7.	**Wyposażenie multimedialne**	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out.
8.	**Obudowa**	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż minimum 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.

		Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować minimum: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz musi być wpisany na stałe w BIOS.
9.	**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 musi doprowadzić do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika musi być 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 musi zapewnić pełną funkcjonalność, a także zachowywać 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.
10.	**BIOS**	BIOS zgodny ze specyfikacją UEFI. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS musi być 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 minimum 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. 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 musi być w stanie 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 minimum 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.
11.	**Wirtualizacja**	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).

12.	**Zgodność z systemami operacyjnymi i standardami**	Oferowane modele komputerów muszą poprawnie współpracować z dostarczonym systemem operacyjnym.
13.	**System operacyjny**	Zainstalowany system operacyjny spełniający następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Licencja bezterminowa zapewniająca prawo do wykorzystywania przez jednostki samorządu terytorialnego. 2. Polska wersja językowa. 3. System operacyjny powinien być dostarczony w najnowszej oferowanej przez producenta wersji. 4. Aktualizacje funkcji dla systemu operacyjnego. 5. Obsługa procesorów wielordzeniowych. 6. Graficzny okienkowy interfejs użytkownika. 7. Obsługa co najmniej 8 GB RAM. 8. Dostęp do aktualizacji w ramach zaoferowanej wersji systemu operacyjnego przez Internet bez dodatkowych opłat. 9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych min.: ● lupa powiększająca zawartość ekranu, ● narrator odczytujący zawartość ekranu, ● regulacja jasności i kontrastu ekranu, ● możliwość odwrócenia kolorów np. biały tekst na czarnym tle, ● poprawa widoczności elementów ekranu np. regulowanie grubości kursora myszy - małej strzałki na ekranie, wskazującej lokalizację myszy i czasu trwania powiadomień systemowych, ● funkcja sterowania myszą z klawiatury numerycznej, ● funkcja klawiszy trwałych, która sprawia, że skrót klawiszowy jest uruchamiany po naciśnięciu jednego klawisza, ● korzystanie z wizualnych rozwiązań alternatywnych wobec dźwięków, ● funkcja napisów w treściach wideo, ● możliwość skorzystania z wizualnych rozwiązań alternatywnych wobec dźwięków; 16. Możliwość zarządzania stacją roboczą poprzez polityki. 17. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 18. Wsparcie dla min. Sun Java i .NET Framework 1.1 i 2.0 i 3.0 i 4.5 – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 19. Wsparcie dla min. JScript i VBScript - możliwość uruchamiania interpretera poleceń. 20. 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. 21. Graficzne środowisko instalacji i konfiguracji. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników. 23. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 24. Oprogramowanie dla tworzenia kopii zapasowych, automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania plików systemowych. Możliwość identyfikacji sieci komputerowych, do których jest podłączony komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
14.	**Certyfikaty i standardy**	Deklaracja zgodności CE (dokument potwierdzający załączyć do formularza ofertowego) Urządzenia muszą być wyprodukowane zgodnie z normą PN-EN ISO 50001 oraz ISO 9001 (dokument potwierdzający załączyć do formularza ofertowego). Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji (wg wytycznych Krajowej Agencji Poszanowania Energii S.A.,

		zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram - dokument potwierdzający załączyć do formularza ofertowego.
15.	**Wymagania dodatkowe**	Wbudowane porty minimum: 2x Display Port 1.4, port audio typu combo (słuchawka/mikrofon) na przednim panelu, port audio-out na tylnym panelu obudowy, 1xRJ-45, 8 portów USB wyprowadzonych na zewnątrz obudowy, w tym min 2 porty USB na przednim panelu obudowy i min. 4 porty USB 3.2 gen. 1 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika). Płyta główna dedykowana dla danego urządzenia, wyposażona minimum w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do min. 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt. SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) Wbudowana nagrywarka DVD +/-RW
16.	**Monitor**	Przekątna matrycy min. 27" Rozdzielczość natywna minimum: Full HD (1080p) 1920 x 1080 przy 75 Hz dla HDMI Jasność minimum: 250 cd/m² Współczynnik kształtu: 16:9 Czas reakcji matrycy minimum: 8 ms (szary-do-szarego, normalny), 5 ms (szary-do-szarego, szybki) Powłoka ekranu: Antyrefleksyjna Złącza wejściowe minimum: 1 x VGA, 1 x HDMI Regulacja pozycji ekranu: Odchylenie
17.	**Ergonomia**	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy jałowej (IDLE) wynosząca maksymalnie 30 dB (załączyć do formularza ofertowego dokument potwierdzający).
18.	**Wsparcie techniczne producenta**	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 (minimum: automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
19.	**Warunki gwarancji**	36 miesięczna gwarancja producenta świadczona na miejscu użytkowania. Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do

		formularza ofertowego. W przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem - dokument potwierdzający załączyć do formularza ofertowego W przypadku awarii, dyski twarde zostają u Zamawiającego – do formularza ofertowego należy załączyć dokument potwierdzający o spełnieniu tego warunku
20.	**Dodatkowe oprogramowanie**	Oprogramowanie zarządzające komputera,umożliwiające min.: - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu - powiadomienie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem. Oprogramowanie producenta z nieograniczoną licencją czasową 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, -możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi, jakiego komponentu sprzętu dotyczy aktualizacja, wszystkich poprzednich aktualizacjach z informacjami jak powyżej. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne. - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr). - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania). - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu min. do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać zestawienie z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. Oprogramowanie biurowe: Wymagane jest dostarczenie stacji wraz z zainstalowanym oprogramowaniem biurowym, które musi mieć zaimplementowane co najmniej następujące funkcjonalności tj. edytor tekstu, arkusz

		kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej i kalendarza, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. Wymagania odnośnie interfejsu użytkownika: a) pełna polska wersja językowa interfejsu użytkownika, b) możliwość zdalnej instalacji pakietu poprzez zasady grup (GPO) w domenie, c) całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie, d) wsparcie dla formatu XML, e) możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów, f) 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, g) możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych, w wypadku nieoczekiwanego zamknięcia aplikacji spowodowanego zanikiem prądu, h) prawidłowe odczytywanie i zapisywanie danych w dokumentach min. w formatach: .DOC, .DOCX, XLS, .XLSX, .PPT, .PPTX, w tym obsługa formatowania, makr, formuł, formularzy w tym plikach wytworzonych w MS Office 2007, MS Office 2010 i MS Office 2013, Office 2016, i) zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). Musi być kompatybilny z posiadanym przez Zamawiającego oprogramowaniem Microsoft Office i pozwalać min. na: a) otwieranie dokumentów utworzonych przy pomocy programów MS Word (od wersji 2007 do 2016), MS Excel (od wersji 2007 do 2016), MS Power Point (od wersji 2007 do 2016), b) w otwieranych dokumentach musi być zachowane oryginalne formatowanie oraz ich treść bez utraty jakichkolwiek ich parametrów i cech użytkowych (min.: korespondencja seryjna, arkusze kalkulacyjne zawierające makra i formularze.) czy też konieczności dodatkowej edycji ze strony użytkownika. Edytor tekstów musi umożliwiać min.: a) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, b) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), c) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, d) automatyczne tworzenie spisów treści, e) sprawdzanie pisowni w języku polskim, f) śledzenie zmian wprowadzonych przez użytkowników, g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, h) określenie układu strony (pionowa/pozioma), i) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego, j) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Arkusz kalkulacyjny musi umożliwiać min.: a) tworzenie raportów tabelarycznych, b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, d) tworzenie raportów z zewnętrznych źródeł danych (min. inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), e) tworzenie raportów tabel przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, f) wykonywanie analiz danych przy użyciu formatowania warunkowego, g) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, h) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, i) formatowanie czasu, daty i wartości finansowych z polskim formatem, j) zapis wielu arkuszy kalkulacyjnych w jednym pliku, k) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 do 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, l) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

		Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać min. przygotowywanie prezentacji multimedialnych oraz: a) drukowanie w formacie umożliwiającym robienie notatek, b) zapisanie w postaci tylko do odczytu, c) nagrywanie narracji dołączanej do prezentacji, d) opatrywanie slajdów notatkami dla prezentera, e) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, f) tworzenie animacji obiektów i całych slajdów. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać min.: a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, c) automatyczne grupowanie poczty o tym samym tytule, d) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, e) oznaczenie poczty elektronicznej z określeniem terminu przypomnienia, f) zarządzanie kalendarzem, g) zapraszanie uczestników na spotkanie, co po ich akceptacji musi spowodować automatyczne wprowadzenie spotkania w ich kalendarzach, h) zarządzanie listą zadań, i) zlecanie zadań innym użytkownikom, j) zarządzanie listą kontaktów, k) udostępnianie listy kontaktów innym użytkownikom, l) przeglądanie listy kontaktów innych użytkowników, m) możliwość przesyłania kontaktów innym użytkowników.

4. Skaner A3 – 1 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry urządzenia
1	2	3
Skaner A3		
1.	Typ skanera (obudowa)	Kompaktowy skaner A3 z automatycznym podajnikiem dokumentów (ADF)
2.	Sposoby skanowania	Simpleks/Dupleks w jednym przebiegu, prosta ścieżka podawania papieru zapewniająca prawidłowe układanie dokumentów po zeskanowaniu na tacy odbiornika
3.	Podajnik Dokumentów	Automatyczny podajnik dokumentów o pojemności co najmniej 100 arkuszy formatu A4 o gramaturze 80 g/m^2 z możliwością regulacji bocznych prowadnic podajnika
4.	Obsługiwane formaty (nie złożone na pół)	Minimum w zakresie A3, A4, A5, A6, B5, B6
5.	Obsługa długich dokumentów	do 550 cm
6.	Gramatura obsługiwanych dokumentów w trybie podawania automatycznego bez korzystania z dodatkowych akcesoriów	30 – 410 g/m^2
7.	Detekcja podwójnych pobrań	Co najmniej jeden czujnik ultradźwiękowy z funkcją automatycznego zachowania obrazu dla umyślnie nałożonych obiektów (takich jak przyklejone notatki lub przymocowane taśmą paragony) zgodnie z ustawionym wzorcem
8.	Ochrona skanowanych dokumentów	Aktywna inteligentna funkcja ochrony dokumentów. Funkcja musi posiadać możliwość włączenia, wyłączenia oraz zmiany stopnia czułości..
9.	Szybkość skanowania (dla dokumentów A4 przy 200 oraz 300 dpi w trybach mono i kolor)	Minimum 60 arkuszy/min., minimum 120 obrazów/min
10.	Typowe dzienne obciążenie skanera	minimum do 15 000 arkuszy (kartek)
11.	Układ optyczny (przetwornik obrazu)	Wykonany min.: w technologii kolorowy CCD (Charge Coupled Device) lub CIS (Contact Image Sensor) - 1 z przodu, 1 z tyłu
12.	Optyczna rozdzielczość skanowania	optyczna 600 dpi, sterownik 1200 dpi
13.	Wyjściowa rozdzielczość skanowania	Minimum 60-600 dpi z możliwością skokowej regulacji co 1 dpi

14.	Tryby koloru skanowania	Monochromatyczny, odcienie szarości, kolor
15.	Obsługiwane systemy operacyjne	Windows 7/10 (32/64-bit) posiadane przez Zamawiającego oraz systemy operacyjne dostarczone ze stacjami roboczymi (dostarczone w ramach niniejszego postępowania)
16.	Interfejsy komunikacyjne	Minimum 1x USB 3.0
17.	Standardy komunikacyjne	Zgodny ze standardem TWAIN oraz ISIS
18.	Funkcje poprawy jakości skanów	Obsługa poniższych funkcjonalności dla zarówno dla standardu TWAIN oraz ISIS: 1) automatyczna poprawa jakości skanowanych dokumentów 2) automatyczne prostowanie i orientacja obrazu 3) automatyczne usuwanie niezadrukowanych stron 4) automatyczna naprawa uszkodzonych lub zagiętych krawędzi dokumentu 5) interaktywna regulacja parametrów skanowania z podglądem na wynik w interfejsie graficznym sterownika z możliwością zapisu ustawień w profilu skanowania 6) skanowanie wielostrumieniowe w jednym przebiegu z możliwością wyboru dowolnej kombinacji trybów koloru 7) łączenie i dzielenie obrazów
19.	Funkcje dołączonego oprogramowania obsługującego standardy TWAIN oraz ISIS	Detekcja i separacja przy pomocy kodów kreskowych min. typu 3z9, ITF, EAN128, NW7, QR Code, Aztec, DataMatrix, PDF417, separacja dokumentów za pomocą niezadrukowanej kartki, odczytaną wartością ze strefy OCR, tzw. "patch code" oraz na podstawie układu formularza, automatyczne nazewnictwo plików za pomocą kodów kreskowych i wartości odczytanej ze strefy OCR z tworzeniem wielopoziomowej struktury katalogów; Obsługiwane formaty plików wyjściowych min. PDF, PDF/A, PDF przeszukiwalny, JPEG, JPEG2000, RTF, TIFF, MTIFF, DOCX, XLSX, PPTX, PNG, BMP. Zapis plików wyjściowych dla poszczególnych strumieni obrazu do oddzielnych folderów na dysku z możliwością wyboru różnych rozszerzeń (formatów) plików, automatyczny odczyt metadanych ze stref OCR i kodów kreskowych z możliwością zapisu min. w jednym z formatów XML, TXT oraz CSV; Obsługiwane metody kompresji plików TIFF min.: CCITT G3, CCITT G4, JBIG, LZW, JPEG oraz plików PDF w celu zredukowania rozmiaru pliku wynikowego; Automatyczne podświetlanie pustych stron i sygnalizacja obrazów o niepewnej jakości w interfejsie użytkownika, możliwość przypisania klawiszy (kombinacji klawiszy) do najczęściej używanych opcji takich jak tworzenie/edycja profilu skanowania, kopiowanie/usuwanie obrazów
20.	Funkcje dołączonego oprogramowania do zarządzania i monitoringu	Działające w strukturze klient-serwer (dwukierunkowa komunikacja wyłącznie w obrębie lokalnej sieci LAN) umożliwiające scentralizowane zarządzanie i monitoring skanera w tym: zdalna aktualizacja sterowników, oprogramowania sprzętowego (firmware) i zdalna konfiguracja ustawień skanerów (na wielu stacjach jednocześnie), generowanie alertów o stanie skanera (błędy) i potrzebie wymiany elementów eksploatacyjnych.
21.	Materiały eksploatacyjne	Materiały eksploatacyjne zainstalowane w skanerze pozwalające na zeskanowanie do min. 200 000 arkuszy
22.	Gwarancja	Minimum 12 miesięcy gwarancji producenta urządzenia

5. Przełącznik zarządzalny – 4 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry urządzenia
1	**2**	**3**
Przełącznik zarządzalny		
1.	Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z wraz z zestawem montażowym rack 19”, wyposażona w zintegrowany zasilacz.
2.	Porty	Minimum 24 portów GigabitEthernet w standardzie BaseT minimum 4 zintegrowane porty 10Gb Ethernet SFP+, minimum 1 port USB.
3.	Wydajność przełącznika	minimum 16000 adresów MAC obsługa minimum 512 wirtualnych sieci możliwość połączenia w stos do 4 urządzeń tego samego typu
4.	Warstwa przełącznika	Minimum L3
5.	Obsługa sieci VLAN	Tak
6.	Certyfikaty i standardy	Zamawiający wymaga aby oferowany przełącznik: - został wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001

		- posiadał deklarację CE
7.	Gwarancja	Min. 12 miesięcy gwarancji producenta

6. Urządzenie do backupu – 1 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry urządzenia
1	**2**	**3**
Urządzenie do backupu		
1.	Procesor	Procesor powinien posiadać min. 4 rdzenie o taktowaniu nie mniejszym niż 2.0 GHz 64bit x86
2.	Pamięć RAM	Nie mniej niż 4GB DDR4
3.	Pamięć RAM liczba slotów	Minimum 2 sloty
4.	Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 16GB
5.	Pamięć Flash	Nie mniej niż 4GB
6.	Liczba zatok na dyski twarde	Minimum 4
7.	Obsługiwane dyski twarde	3.5" oraz 2.5" SATA oraz 2.5" SATA SSD
8.	Pojemność dysków twardych	Możliwość rozbudowy o do łącznej pojemności minimum 18TB
9.	Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
10.	Zainstalowane dyski twarde	Minimum 2 dyski o pojemności minimum 4TB
11.	Porty LAN 2,5 GbE	Minimum 2
12.	Diody LED	Minimum Status, LAN, HDD,
13.	Porty USB 3.2 Gen 2	Minimum 2
14.	Porty USB 2.0	Minimum 2
15.	Port PCiE	Tak, minimum 1 Gen3
16.	Przyciski	Reset, Zasilanie
17.	Typ obudowy	RACK, minimum 1U
18.	Dopuszczalna temperatura pracy	od 0 do 40˚C
19.	Wilgotność względna podczas pracy	5-95% R.H.
20.	Zasilanie	Zasilacz max. 250 W, 100-240 V
21.	Agregacja łączy	Tak
22.	Obsługiwane systemy plików	Dyski wewnętrzne min.: EXT4 Dyski zewnętrzne min.: EXT3, EXT4, NTFS, FAT32, HFS+
23.	Możliwość podłączenia karty WLAN na USB	Tak
24.	Szyfrowanie wolumenów	Tak, min AES 256
25.	Szyfrowanie dysków zewnętrznych	Tak
26.	Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
27.	Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
28.	Zarządzanie prawami	Ograniczenie dostępnej pojemności dysku dla użytkownika

	dostępu	Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
29.	Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
30.	Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows posiadanych przez Zamawiającego oraz systemów operacyjnych które zostaną dostarczone z serwerem i stacjami roboczymi o których mowa powyżej: , backup na zewnętrzne dyski twarde,
31.	Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
32.	VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN
33.	Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu
34.	Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych min. na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki internetowej Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
35.	Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów min. dla LXC i Docker
36.	Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach min. za pośrednictwem Email i SMS
37.	Wyposażenie dodatkowe	Szafa rack minimum 42U, minimum 600x1000mm
38.	Gwarancja	Minimum 36 miesięcy świadczonych przez producenta sprzętu

7. UPS – 1 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry urządzenia
1	**2**	**3**
UPS		
1.	moc pozorna	minimum 1200VA
2.	moc rzeczywista	minimum 750W
3.	Technologia	VI (line interactive)
4.	Typ obudowy	RACK 19"

5.	Zakres napięcia wejściowego	~168V – 264V ± 2%
6.	Kształt napięcia wyjściowego	Taki jak na wejściu
7.	Automatyczna regulacja napięcia (AVR)	Wymagane na poziomie min. +/- 10%
8.	Czas przełączania sieć – UPS	<3ms
9.	Filtracja napięcia wyjściowego	Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy
10.	Napięcie wyjściowe	~230V ± 5%
11.	Częstotliwość napięcia wyjściowego	50Hz ± 1Hz
12.	Kształt napięcia wyjściowego na pracy bateryjnej	Sinus
13.	Zabezpieczenie przeciwzwarciowe	elektroniczne
14.	Zabezpieczenie przeciążeniowe	elektroniczne
15.	Czas podtrzymania (P0,8max/P0,5max)	minimum 4 min / 7 min
16.	Przeciążalność	>105% - 3s
17.	Akumulatory wewnętrzne	minimum 2 szt 12V5Ah; szczelne, bezobsługowe
18.	Wejście zasilania	przewód podłaczony na stałe do UPS'a zakończony wtyczką unischuko z uziemieniem 16A
19.	Ilość i typ gniazd wyjściowych	minimum 5 gniazd z podtrzymaniem z czego minimum 2 gniazda standardu polskiego
20.	Interfejs komunikacyjny	USB HID, Wykonawca powinien dostarczyć kabel
21.	Szyny / wsporniki motażowe RACK	wymagane
22.	Waga UPS	do 15 kg
23.	Gwarancja	Minimum 36 miesięcy na elektronikę i minimum 24 miesięcy na akumulatory. Wymagane wsparcie producenta (telefoniczne oraz mailowe) odnośnie konfiguracji i rozwiązywania problemów. Serwis powinien być realizowany w systemie door-to-door. ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania **- należy dołączyć do oferty dokument potwierdzający spełnienie wymagań.**

8. Audyt cyberbezpieczeństwa – 1 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry audytu
1	**2**	**3**
Audyt cyberbezpieczeństwa		
1.	**Typ**	Wykonanie audytu diagnozy cyberbezpieczeństwa, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do dokumentacji konkursowej - Cyfrowa Gmina. 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/SkrytkaESP.
2.	**Plan audytu**	Audyt musi składać się z minimum: 1. Audyt dokumentacji i procesów: - ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC) - ocena wybranych aspektów bezpieczeństwa systemów informatycznych

		- ocena dojrzałości wybranych procesów bezpieczeństwa - opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny 2. Testy penetracyjne infrastruktury sieciowej - Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci - skanowanie sieci, rekonesans sieci (skanowanie musi zostać powtórzone dla każdej wskazanej przez Zamawiającego sieci) - skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), który zostały wybrane na podstawie wcześniejszej analizy - sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy - sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł - weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych - weryfikacja zabezpieczeń urządzeń sieciowych - testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej - wykonanie raportu zawierającego minimum: ● opis wszystkich elementów, które zostały poddane audytowi ● podział podatności ze względu na ryzyko: wysoki, średni, niski ● wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności ● wylistowanie wszystkich podatności ze względu na ryzyko: wysoki, średni, niski ● określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności - Wsparcie poaudytowe - Udzielenie informacji na temat audytowanych elementów wynikających z raportu. Czas na zapoznanie się z raportem i zadawanie pytań odnośnie raportu.
3.	**Wymagania dla audytora/-ów**	Audyt musi zostać przeprowadzony przez osobę/-y posiadająca/-e uprawnienia wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu: 1. Certified Internal Auditor (CIA); 2. Certified Information System Auditor (CISA); 3. 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; 4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób; 5. Certified Information Security Manager (CISM); 6. Certified in Risk and Information Systems Control (CRISC); 7. Certified in the Governance of Enterprise IT (CGEIT); 8. Certified Information Systems Security Professional (CISSP); 9. Systems Security Certified Practitioner (SSCP);

		10. Certified Reliability Professional; 11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

9. Urządzenie klasy UTM – 1 szt.

Lp.	Wymagane minimalne parametry urządzenia
1	**2**
Urządzenie klasy UTM	
Obsługa sieci	
1.	Urządzenie powinno 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.
Zapora (Firewall)	
2.	Urządzenie powinno być wyposażone w Firewall klasy Stateful Inspection.
3.	Urządzenie powinno obsługiwać translacje minimum adresów NAT n:1, NAT 1:1 oraz PAT.
4.	Urządzenie powinno dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5.	Interface (GUI) do konfiguracji firewall powinien umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca powinna mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6.	Administrator powinien mieć możliwość budowania reguł firewall minimum na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7.	Urządzenie powinno umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8.	Administrator powinien mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9.	Edytor reguł firewall powinien posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10.	Urządzenie powinno umożliwiać uwierzytelnienie i autoryzację użytkowników minimum w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11.	Urządzenie powinno umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
Intrusion Prevention System (IPS)	
12.	System detekcji i prewencji włamań (IPS) powinien być zaimplementowany w jądrze systemu i powinien wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
13.	Moduł IPS powinien być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy
14.	Moduł IPS powinien zabezpieczać przed co najmniej 10 000 ataków i zagrożeń
15.	Administrator powinien mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
16.	Moduł IPS powinien nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
17.	Urządzenie powinno umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
18.	Administrator powinien 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.
19.	Urządzenie powinno umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
Kształtowanie pasma (Traffic Shapping)	
20.	Urządzenie powinno umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
21.	Ograniczenie pasma lub priorytetyzacja reguły firewall powinno być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
22.	Urządzenie powinno umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
23.	Urządzenie powinno umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	
24.	Urządzenie powinno umożliwiać zastosowanie co najmniej jednego skanera antywirusowego dostarczanego przez firmy trzecie (inne niż producent rozwiązania).
25.	Co najmniej jeden z dwóch skanerów antywirusowych powinien być dostarczany w ramach podstawowej licencji.

26.	Administrator powinien mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
27.	Administrator powinien 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 powinien być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	
28.	Urządzenie powinno posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
29.	Ochrona antyspam powinien działać min. w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny.
30.	W przypadku ochrony w oparciu o DNS RBL administrator powinien mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
31.	Wpis w nagłówku wiadomości zaklasyfikowanej jako spam powinien być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (VPN)	
32.	Urządzenie powinno umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
33.	Urządzenie powinno wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN.
34.	SSL VPN powinien działać co najmniej w trybach tunelu i portalu.
35.	Producent urządzenia powinien umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
36.	Urządzenie powinno umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
37.	Urządzenie powinno umożliwiać wsparcie minimum dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
38.	Urządzenie powinno umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
Filtr dostępu do stron WWW	
39.	Urządzenie powinno posiadać wbudowany filtr URL.
40.	Filtr URL powinien działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
41.	Administrator powinien mieć możliwość dodawania własnych kategorii URL.
42.	Administrator powinien mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
43.	Administrator powinien mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
44.	Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
45.	Filtr URL musi uwzględniać komunikację po protokole HTTPS.
46.	Urządzenie powinno umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
47.	Urządzenie powinno umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
Uwierzytelnianie	
48.	Urządzenie powinno umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory.
49.	Urządzenie powinno umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
50.	Urządzenie powinno umożliwiać uruchomienie specjalnego portalu (captive portal), który powinien zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos.
51.	Urządzenie powinno umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
52.	Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
53.	Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
Administracja łączami do internetu (ISP)	
54.	Urządzenie powinno umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
55.	Mechanizm równoważenia obciążenia łącza internetowego powinien działać w oparciu o min. następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego,

	b. równoważenie względem połączenia.
56.	Mechanizm równoważenia obciążenia powinien uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
57.	Urządzenie powinno umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
58.	Urządzenie powinno wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
59.	W zakresie SD-WAN urządzenie powinno zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
60.	Monitorowanie dostępności łącza musi być możliwe min. w oparciu o ICMP oraz TCP.
ROUTING (TRASOWANIE)	
61.	Urządzenie powinno umożliwiać statyczne trasowanie pakietów.
62.	Urządzenie powinno umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
63.	Urządzenie powinno umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
64.	Urządzenie powinno umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
Administracja urządzeniem	
65.	Konfiguracja urządzenia powinna być możliwa z wykorzystaniem polskiego interfejsu graficznego.
66.	Interfejs konfiguracyjny powinien być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
67.	Administrator powinien mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
68.	Urządzenie powinno umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
69.	Urządzenie powinno umożliwiać zarządzanie z poziomu konsoli (SSH)
70.	Urządzenie powinno umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
71.	Interfejs konfiguracyjny platformy centralnego zarządzania powinien być dostępny poprzez przeglądarkę internetową, a komunikacja powinna być zabezpieczona za pomocą protokołu HTTPS.
72.	Urządzenie powinno umożliwiać zapisywanie logów na wbudowanym dysku.
73.	Urządzenie powinno umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
74.	Urządzenie powinno umożliwiać eksportowanie logów minimum za pomocą protokołu IPFIX.
75.	Urządzenie powinno umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
76.	Urządzenie powinno umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
77.	Urządzenie powinno umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
Raportowanie	
78.	Urządzenie powinno posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
79.	System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
80.	System raportowania powinien posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
81.	System raportowania powinien umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
82.	W ramach posiadanej licencji urządzenie powinno umożliwiać skorzystanie z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
83.	Urządzenie powinno umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
84.	Urządzenie powinno umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
POZOSTAŁE WYMAGANE USŁUGI I FUNKCJE	
85.	Urządzenie powinno posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
86.	Urządzenie powinno pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
87.	Konfiguracja serwera powinna być niezależna dla IPv4 i IPv6.
88.	Urządzenie powinno umożliwiać stworzenie różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
89.	Urządzenie powinno posiadać usługę DNS Proxy.
90.	Urządzenie powinno posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu powinno być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
Parametry sprzętowe	
91.	Urządzenie powinno być pozbawione dysku twardego, a oprogramowanie wewnętrzne powinno działać na wbudowanej pamięci flash.

92.	Urządzenie powinno umożliwiać podłączenie karty SD w celu zapisywania logów.
93.	Liczba portów Ethernet 10/100/1000Mbps – min.5.
94.	Urządzenie powinno umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
95.	Przepustowość Firewall (1518 bajtów UDP) – minimum 1Gbps.
96.	Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1Gbps.
97.	Przepustowość filtrowania Antywirusowego – minimum 260Mbps.
98.	Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 200Mbps.
99.	Maksymalna liczba tuneli VPN IPSec – minimum 50.
100.	Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 5.
101.	Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 20.
102.	Obsługa interfejsów 802.11q (VLAN) – minimum 128
103.	Liczba równoczesnych sesji – minimum 150 000 i nie mniej niż 6 000 nowych sesji/sekundę.
104.	Urządzenie nie powinno mieć limitu na liczbę użytkowników.
105.	Liczba reguł filtrowania – minimum 4 096.
106.	Liczba tras statycznego routingu – minimum 512.
107.	Liczba tras dynamicznego routingu – minimum 1 000.
Gwarancja i serwis	
108.	Urządzenie powinno być objęte min 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
109.	W okresie obowiązywania gwarancji powinno być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

10. Certyfikowane szkolenie dla administratora z dostarczonych rozwiązań oraz z zakresu cyberbezpieczeństwa – 1 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry szkolenia
1	2	3
Certyfikowane szkolenie dla administratora z dostarczonych rozwiązań oraz z zakresu cyberbezpieczeństwa		
1.	**Typ**	Szkolenie stacjonarne dla administratora z zakresu dostarczonego urządzenia klasy UTM wraz z egzaminem
2.	**Program szkolenia**	1. Rozpoczęcie pracy z urządzeniem ● Wprowadzenie do interfejsu administracyjnego ● Ustawienia systemowe i uprawnienia administratorów ● Instalacja licencji i aktualizacja systemu ● Tworzenie kopii zapasowej i przywracanie konfiguracji 2. Zbieranie logów i monitorowanie ● Przedstawienie kategorii zbieranych logów ● Wykresy historyczne i monitorowanie 3. Obiekty ● Typy obiektów oraz ich wykorzystanie ● Obiekty sieciowe i obiekt typu „router” 4. Konfiguracja sieci ● Tryby pracy urządzenia ● Typy interfejsów (Ethernet, modem, bridge, VLAN, GRETAP) ● Typy routingu oraz ich priorytety 5. Translacja adresów sieciowych (NAT) 6. Translacja połączeń wychodzących (maskarada) 7. Translacja połączeń przychodzących (przekierowanie) 8. Translacja dwukierunkowa (jeden do jeden) 9. Filtrowanie ruchu sieciowego (Firewall) 10. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection) ● Szczegółowy opis parametrów reguły Firewall ● Kolejność przetwarzania reguł Firewall i NAT 11. Ochrona aplikacji ● Implementacja filtrowania URL dla ruchu http i https ● Konfigurowanie skanowania antywirusowego i modułu Breach Fighter ● Moduł IPS i stosowanie profili inspekcji 12. Użytkownicy i uwierzytelnianie 13. Konfiguracja usługi katalogowej ● Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius,

		certyfikat SSL, SPNEGO, SSO) ● Rejestracja użytkowników ● Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania 14. Wirtualne sieci prywatne (VPN) ● Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2) ● Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK) ● Tunele VTI 15. SSL VPN ● Zasada działania ● Konfiguracja
3.	**Wymagania dodatkowe**	W ramach realizacji szkolenia wymagane jest, aby: - Szkolenie stacjonarne, realizowane przez autoryzowane centrum szkoleniowe przez producenta dostarczonego urządzenia klasy UTM, w miejscu oddalonym nie więcej niż 300 km od Gminy Wiejskiej Gubin - Uczestnik szkolenia musi mieć zapewnione wyżywienie (min. śniadanie, lunch oraz przerwy kawowe w trakcie trwania szkolenia) - Uczestnik szkolenia musi mieć zapewniony nocleg na min. 2 doby, w miejscu oddalonym nie dalej niż 10 km od miejsca szkolenia - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych, - Uczestnik po zakończeniu szkolenia musi otrzymać zaświadczenie ukończenia szkolenia - Uczestnik po zakończeniu szkolenia musi mieć prawo do bezpłatnego odbycia autoryzowanego przez producenta dostarczonego urządzenia klasy UTM, egzaminu - Uczestnik musi mieć możliwość bezpłatnego 14-sto dniowego kontaktu z trenerem po szkoleniu.

11. Szkolenie dla pracowników z zakresu cyberbezpieczeństwa – 1 kpl.

Lp.	Nazwa komponentu	Wymagane minimalne parametry szkolenia
1	**2**	**3**
Szkolenie dla pracowników z zakresu cyberbezpieczeństwa		
1.	**Typ**	Szkolenie zdalne dla pracowników Urzędu z zakresu cyberbezpieczeństwa
2.	**Wymagany minimalny zakres 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 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 - HTTP FTP 14. Zaszyfrowana komunikacja w Internecie (komunikatory) 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. Podpis elektroniczny dokumentów w prosty i bezpieczny sposób.
3.	**Wymagania dodatkowe**	W ramach realizacji szkolenia wymagane jest, aby: - Szczegółowy harmonogram szkolenia został uzgodniony z Zamawiającym terminie minimum 14 dni przed terminem rozpoczęcia szkolenia - Szkolenia zostaną 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.
4.	**Ilość**	Szkolenie dla 30 pracowników

12. Równoważność rozwiązań

Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych rozwiązaniom wskazanym przez Zamawiającego. Wykonawca oferując rozwiązanie równoważne do opisanego powyżej jest zobowiązany wykazać (udowodnić) równoważność w zakresie wskazanych parametrów, które muszą być na poziomie nie gorszym niż parametry wskazane przez Zamawiającego - Wykonawca musi wykazać (udowodnić), iż proponowane rozwiązanie w równoważnym stopniu spełnia wymagania określone w zapytaniu ofertowym, w szczególności w zakresie parametrów. Jeżeli w opisie przedmiotu zamówienia znajdują się jakiekolwiek odniesienia do określonego wyrobu, źródła, znaków towarowych, patentów czy pochodzenia lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę – należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza składanie ofert równoważnych, w szczególności o parametrach technicznych, użytkowych, funkcjonalnych i jakościowych nie gorszych niż te, podane w opisie przedmiotu zamówienia. Ilekroć Zamawiający przy opisie przedmiotu zamówienia powołuje się na normy, aprobaty, specyfikacje techniczne czy systemy odniesienia Zamawiający dopuszcza rozwiązania równoważne. Jeżeli w opisie przedmiotu zamówienia znajdują się jakiekolwiek odniesienia do wielkości fizycznych ciała lub zjawiska, którą można określić ilościowo, czyli zmierzyć za pomocą jednostki miary (o ile nie wskazano inaczej) – należy przyjąć, iż jako równoważne Zamawiający uzna ofertę, która uwzględni wymiary wraz z dopuszczonymi odchyleniami od wymiarów podanych w zapytaniu ofertowym mieszczące się w granicach tolerancji określonych normą/standardem, dla której/którego wypracowano system normalizacji i certyfikacji na poziomie co najmniej międzynarodowym. Norma/standard musi być obowiązujący wg przepisów prawa na dzień wyceny. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego jest obowiązany wykazać (udowodnić), że oferowany przez niego produkt spełnia wymagania określone przez Zamawiającego w zapytaniu ofertowym.