Znak sprawy: GG.271.9.2022.WK

Załącznik nr 4

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Wymagania ogólne dla urządzeń i oprogramowania.

1. Dostarczony sprzęt musi być fabrycznie nowy (wyprodukowany nie wcześniej niż 6 miesięcy przed dostawą), nieużywany, wolny od wad, wykonany w ramach bezpiecznych technologii oraz wolny od obciążeń prawami osób trzecich, a także musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej.
2. Oferowany sprzęt musi reprezentować model bieżącej linii produkcyjnej. Zamawiający nie dopuszcza dostawy urządzeń odnawianych (refurbished), demonstracyjnych lub powystawowych.
3. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy urządzeń, w szczególności podzespoły montowane przez producenta były przez niego certyfikowane. Wykonawca nie będący producentem oferowanego sprzętu nie może samodzielnie dokonywać modyfikacji sprzętu i wprowadzać zmian w fabrycznej konfiguracji. Zamawiający nie dopuszcza dostawy urządzeń modyfikowanych przez sprzedawcę oraz nie dopuszcza modyfikacji na linii produkcyjnej dystrybutora.
4. Dostarczone wraz ze sprzętem oprogramowanie musi być opatrzone we wszystkie atrybuty oryginalności i legalności, wymagane przez producenta oprogramowania w zależności od dostarczanej wersji.
5. Zamawiający zastrzega sobie prawo do weryfikacji dostarczonego sprzętu na etapie dostawy, również pod kątem legalności oprogramowania. W ramach procedury odbioru, Zamawiający zastrzega sobie prawo do przeprowadzenia weryfikacji legalności i oryginalności zainstalowanego oprogramowania bezpośrednio u producenta oprogramowania, przed podpisaniem protokołu odbioru w sposób, który uzna za bezsporny.
6. W przypadku wykrycia, że zainstalowany system operacyjny nie jest nowy, był już używany lub był już wcześniej aktywowany Zamawiający odmówi przyjęcia sprzętu i wezwie Wykonawcę do usunięcia nieprawidłowości w wyznaczonym terminie.

II. Wymagania gwarancyjne.

Sprzęt

1. Na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta sprzętu lub oparta na gwarancji autoryzowanego serwisu producenta, z czasem reakcji na zgłoszony na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie przekraczającym jednego dnia roboczego (chyba że zapisy szczegółowe stanowią inaczej).

Znak sprawy: GG.271.9.2022.WK

2. Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.

Oprogramowanie

1. Oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej).

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części OPZ.

III. Miejsce uruchomienia systemu informatycznego (instalacji sprzętu i oprogramowania).

Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części OPZ, w budynku urzędu w miejscu wskazanym przez Zamawiającego.

IV. Zestawienie zakresu dostaw i usług.

Lp.	Nazwa dostawy/usługi	Ilość	Opis
1	Stacje robocze	3 szt.	Stacja robocza wraz z systemem operacyjnym będzie wykorzystywana do realizacji usług publicznych, procedowania dokumentów, dla potrzeb aplikacji biurowych, obliczeniowych, w celu dostępu do Internetu oraz poczty elektronicznej.
2	Pakiet oprogramowania biurowego	3 szt.	Zbiór programów komputerowych służących do typowych zastosowań biurowych, takich jak edycja tekstu, wykonywanie obliczeń księgowych, czy tworzenie i obsługa prezentacji, które mają zostać dostarczone jako jeden zintegrowany produkt.
3	Monitory LCD	3 szt.	Dostawa monitorów ekranowych LCD do nowych stacji roboczych
4	Serwer z systemem operacyjnym	1 szt.	Dostawa fizycznego serwera wraz z serwerowym systemem operacyjnym i licencjami dostępowymi, który zostanie wykorzystany do uruchomienia i udostępniania usług koniecznych do funkcjonowania urzędu.

Znak sprawy: GG.271.9.2022.WK

5	Serwer backupowy	1 szt.	Dostawa serwera NAS stanowiącego serwer backupowy, dzięki któremu możliwe będzie wykonywanie bezpiecznych, integralnych kopii zapasowych.
6	Tworzenie domen platform portali tylko związane z cyberbezpieczenstwem i dostosowaniem do WCAG 2.1	1 usł	Wykonanie modernizacji strony internetowej urzędu. Wobec wymagań związanych z dostępnością cyfrową dla podmiotów publicznych strona internetowa urzędu zostanie zmodernizowana w taki sposób, aby osiągnąć zgodność ze strukturą WCAG 2.1
7	Rozbudowa zabezpieczeń logicznych (firewall, IDS, IPS)	1 szt.	Dostawa systemu firewall jako głównego elementu chroniącego dostęp do zasobów sieciowych. Zakup profesjonalnej zapory sieciowej zapewni ochronę przed cyberatakami z zewnątrz, zabezpieczy również lokalną sieć wraz z wszystkimi urządzeniami, które się w niej znajdują.
8	Usługi informatyczne z zakresu wdrożenia konserwacji i serwisu sprzętu informatycznego oraz oprogramowania	1 usł	Usługa instalacji i konfiguracji, migracji danych, na nowe rozwiązanie teleinformatyczne, szkolenia administratora (instruktaż stanowiskowy) wraz wsparciem technicznym.
9	Diagnoza cyberbezpieczeństwa	1 usł	Usługa dotyczy przeprowadzenia diagnozy cyberbezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina".

V. Szczegółowy opis wymagań minimalnych dla urządzeń i systemów teleinformatycznych.

1. Stacje robocze

Minimalne wymagania podstawowe dla stacji roboczej z oprogramowaniem	
Parametr	**Charakterystyka (wymagania minimalne)**
Typ	Stacja robocza z systemem operacyjnym. W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanej stacji roboczej.
Funkcjonalność obudowy	1. Wymagana obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej, typu Small Form Factor z obsługą kart wyłącznie o niskim profilu, umożliwiająca montaż dysku w formacie 3,5" lub 2,5" wewnątrz obudowy. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25" typu slim.

Znak sprawy: GG.271.9.2022.WK

	2. 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 powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco - diagnostycznym. 3. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej. 4. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie wpisanym na stałe w BIOS.
Zasilacz	Zasilacz o mocy max. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Oferowany zasilacz w oferowanym komputerze musi spełniać wymóg 80 Plus (80+).
Procesor	Wymagany procesor klasy x86 wielordzeniowy, przystosowany na etapie produkcji do pracy w komputerach stacjonarnych, umożliwiający osiągnięcie w teście Passmark CPU Mark, w kategorii Average CPU Mark wyniku min. 12000 punktów. Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony www.cpubenchmark.net
Funkcjonalność płyty głównej	1. Płyta główna dedykowana dla oferowanej stacji roboczej , wyposażona w co najmniej w: 1x PCIe x16 Gen.3, 1x PCIe x1, 2x SATA w tym min. 1 szt SATA 3.0, jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej oraz wyposażona w co najmniej w: 2 gniazda DIMM do montażu pamięci RAM 2. Płyta główna wyposażona w dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania zaimplementowany w taki sposób, że próba usunięcia układu spowoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w chipsecie na płycie głównej.
Pamięć	Co najmniej 8 GB pamięci RAM z możliwością rozbudowy do min. 64 GB Co najmniej 512 GB - wymagany dysk w technologii półprzewodnikowej SSD (Solid State Drive)
Układ graficzny	Wymagany układ graficzny, umożliwiający osiągnięcie w teście Passmark Average G3D Mark wyniku min. 790 punktów.

Znak sprawy: GG.271.9.2022.WK

	Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony www.videocardbenchmark.net
Wyposażanie multimedialne	Dwukanałowa karta dźwiękowa zgodna ze standardem High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie typu combo, na tylnym panelu min. port audio line out
Bezpieczeństwo	Wymagany komputer z systemem służącym diagnostyce wyposażonym w graficzny interfejs użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera, a w szczególności jego składowych. System musi zapewnić pełną funkcjonalność, w szczególności zachować interfejs graficzny nawet w przypadku braku dysku twardego (lub jego uszkodzenia), nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do Internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
System diagnostyczny	Zamawiający wymaga zaoferowania stacji roboczej wyposażonej fabrycznie w wbudowany wizualny system diagnostyczny oparty o sygnalizację LED, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami - sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). Zamawiający wymaga aby system był usytuowany na przednim panelu obudowy i sygnalizował co najmniej następujące stany: 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.
BIOS	Wymagany BIOS zgodny ze specyfikacją UEFI, zawierający informację o nazwie producenta komputera lub nazwie modelu oferowanego komputera. Wymagana pełna obsługa BIOS za pomocą klawiatury i myszy jak również samej myszy. BIOS musi być wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności dla następujących zmian: procesora, wielkości pamięci oraz pojemności dysku. Wymagana możliwość odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej

	prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio - realizowana bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych. Do odczytu wskazanych powyżej informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, itp. system diagnostyczny, czy dodatkowe oprogramowanie. W ramach BIOS wymagana jest funkcjonalność polegająca na blokowaniu/ odblokowaniu BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora - użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Wymagana możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Wymagana możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB), możliwość wyłączania portów USB pojedynczo. Wymagana możliwość nadania numeru inwentarzowego bezpośrednio z poziomu BIOS (bez wykorzystania dodatkowego oprogramowania), składającego się liter, cyfr oraz znaków specjalnych - wpisany numer inwentarzowy ma nie ulegać skasowaniu po aktualizacji BIOS. Wymagana 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 itp.: 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 oraz upgrade BIOS.
Wirtualizacja	Wymagane 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).

Znak sprawy: GG.271.9.2022.WK

Certyfikaty i standardy	1) spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. 2) Spełnienie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. 3) Spełnienie normy ISO 50001 lub równoważnej dla producenta sprzętu w zakresie produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. 4) Oferowany sprzęt musi posiadać oznaczenie CE 5) Wymagany certyfikat EnergyStar 6) Wymagany Certyfikat TCO
Porty I/O	Stacja robocza wyposażona w następujące wbudowane gniazda (porty I/O): 1. Minimum 2 wyjścia cyfrowe video (w tym, co najmniej 1x DisplayPort 1.4) 2. Minimum 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: a. Panel przedni: minimum 2x USB 2.0 b. Panel tylny: minimum 4x USB 3.2 gen 1 Typu A oraz 2x USB 2.0 3. 1x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu 4. 1x port audio-out na tylnym panelu obudowy 5. 1x RJ-45 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.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 26 dB.
Oprogramowanie dodatkowe	Dołączone do oferowanego komputera oprogramowanie dodatkowe z nieograniczoną licencją czasową na użytkowanie umożliwiające realizację następujących funkcjonalności: 1. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, 2. możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu

Znak sprawy: GG.271.9.2022.WK

	połączenia internetowego z automatycznym przekierowaniem, a w szczególności informacji o: a. poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. 3. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne. 4. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. 5. rozpoznanie modelu oferowanego komputera, numeru seryjnego komputera, informacji kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem dokładnej daty (dd-mm-rrrr) 6. sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) 7. dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml 8. 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 do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datę (dd-mm-rrrr) i godzinę z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. Zamawiający oczekuje dostawy stacji roboczej wyposażonej w oprogramowanie zarządzające wyposażone co najmniej w następujące funkcjonalności: 1. monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów 2. powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu 3. powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów

Znak sprawy: GG.271.9.2022.WK

	4. śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.
Komunikacja	1. Karta sieciowa przewodowa 10/100/1000 na wtyk RJ-45, wspierająca obsługę WoL (funkcja włączana przez użytkownika) 2. Karta sieciowa bezprzewodowa pracująca w standardzie Wi-Fi 6 802.11ax, Dual-band 2x2 MU-MIMO 3. Bluetooth 5.1
Peryferia	1. Klawiatura w układzie polski programisty. 2. Mysz optyczna z dwoma przyciskami i rolką.
System operacyjny	Bezterminowa licencja oprogramowania systemu operacyjnego klasy Microsoft Windows 11 Professional lub równoważny. Za równoważny system operacyjny Zamawiający uzna system spełniający następujące minimalne parametry: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet; Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; 2. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; 3. Internetowa aktualizacja zapewniona w języku polskim; 4. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 5. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6; 6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe; 7. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); 8. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 9. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; 10. Praca systemu w trybie ochrony kont użytkowników; 11. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; 12. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;

Znak sprawy: GG.271.9.2022.WK

	13. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; 14. Aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; 15. Wbudowany system pomocy w języku polskim; 16. System operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 17. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; 18. System posiadać powinien narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 19. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; 20. Graficzne środowisko instalacji i konfiguracji; 21. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; 22. Możliwość przywracania plików systemowych; 23. Możliwość „downgrade" do niższej wersji. System musi być nowy (nie aktywowany wcześniej na innym urządzeniu), zainstalowany fabrycznie na dostarczonym komputerze przez producenta sprzętu.
Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta	W ramach wsparcia serwisowego producenta wymagany jest dedykowany portal techniczny prowadzony przez producenta lub na jego zlecenie (z bezpłatnym dostępem) służący m.in. do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. Portal musi oferować możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego, a także możliwość pobrania aktualnych wersji sterowników oraz firmware dla stacji roboczej również w przypadku wygaśnięcia wsparcia technicznego. Portal musi mieć możliwość sprawdzenia oraz dostarczenia kompletnych danych o urządzeniu co najmniej w następującym zakresie: automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego.

Znak sprawy: GG.271.9.2022.WK

	Dla zaoferowanej stacji roboczej Zamawiający wymaga następujących warunków gwarancji i serwisu: 1. Minimalny czas trwania gwarancji udzielonej przez producenta na stację roboczą wynosi 60 miesięcy (5 lat). 2. Zamawiający wymaga gwarancji uwzględniającej zabezpieczenie serwisowe, które w przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, umożliwi pozostawienie uszkodzonego dysku u Zamawiającego (dysk nie będzie podlegał ekspertyzie poza siedzibą Zamawiającego) - przed podpisaniem umowy Zamawiający będzie żądał przedłożenia przez Wykonawcę oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku. 3. Okres zabezpieczenia serwisowego na dyski twarde, o którym mowa w pkt 2 musi być tożsamy z czasem gwarancji udzielonej na stację roboczą, w szczególności przy zaoferowaniu rozszerzenia gwarancji podstawowej. Wymagana gwarancja producenta świadczona na miejscu u klienta (w przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez dział wsparcia technicznego). Wymagany czas reakcji serwisu na zgłoszenie - do końca następnego dnia roboczego. Firma serwisująca musi posiadać wdrożoną normę ISO 9001 lub równoważną na świadczenie usług serwisowych oraz posiadać autoryzacje producenta stacji roboczej - dokumenty potwierdzające załączyć do oferty.

2. Licencja na pakiet oprogramowania biurowego (edytor tekstu, arkusz kalkulacyjny, narzędzie do przygotowania prezentacji)

Wymagania minimalne
1) W ramach licencji wieczystej (bezterminowej) oprogramowanie musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: a. Dostępność pakietu w wersjach 32-bit oraz 64-bit, stały dostęp do najnowszych aktualizacji zakupionej wersji oprogramowania. 2) Wymagania odnośnie interfejsu użytkownika: a. Pełna polska wersja językowa interfejsu użytkownika.

b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

3) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
   a. Posiada kompletny i publicznie dostępny opis formatu,
   b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526 ze zm.),
   c. Umożliwia kreowanie plików w formacie XML,
   d. Wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,
4) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
5) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
6) Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a. Edytor tekstów,
   b. Arkusz kalkulacyjny,
   c. Narzędzie do przygotowywania i prowadzenia prezentacji.

   Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
7) Arkusz kalkulacyjny musi umożliwiać:
   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 (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
   e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
   f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
   g. Wyszukiwanie i zamianę danych.
   h. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
   i. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS.
   j. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
   k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
   l. Formatowanie czasu, daty i wartości finansowych z polskim formatem.

m. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
n. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
o. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013, 2016, 2019, 365 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
p. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

8) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a. Przygotowywanie prezentacji multimedialnych, które będą:
- Prezentowanie przy użyciu projektora multimedialnego .
- Drukowanie w formacie umożliwiającym robienie notatek.
b. Zapisanie, jako prezentacja tylko do odczytu.
c. Nagrywanie narracji i dołączanie jej do prezentacji.
d. Opatrywanie slajdów notatkami dla prezentera.
e. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
f. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
g. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
h. Możliwość tworzenia animacji obiektów i całych slajdów.
i. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
j. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013, 2016, 2019 i 365.

9) Wymagana jest dostawa pakietu w najnowszej dostępnej na rynku wersji jako produkt fizyczny z przyporządkowaniem 1 licencja = 1 komputer.

3. Monitory ekranowe LCD

Minimalne wymagania podstawowe dla monitorów ekranowych LCD	
Parametr	**Charakterystyka (wymagania minimalne)**
Typ	Monitor ekranowy LCD. W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego monitora.
Ekran	1. Wyświetlacza LCD z podświetleniem LED 2. Typu panela IPS, wyposażony w powłokę antyodblaskową

Znak sprawy: GG.271.9.2022.WK

	3. Przekątna min. 27'' w formacie 16:9 4. Pracujący w rozdzielczości 1920x1080 5. Jasność: min. 300 cd/m² 6. Czas reakcji: 8 ms (gray-to-gray) 7. Kontrast: 1000:1 8. Kąty widzenia 178 stopni w pionie i 178 stopni w poziomie
Złącza video	Minimum jedno złącze cyfrowe video zgodnie ze złączem w oferowanym komputerze, w zestawie okablowanie do podłączenia z oferowanym komputerem.
Funkcjonalność obudowy	1. Możliwość pochylenia ekranu w zakresie -5/+21 stopni. 2. Możliwość montażu na ścianie lub za pomocą dedykowanego uchwytu z wykorzystaniem standardu VESA. 3. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej.
Certyfikaty i standardy	Oferowany sprzęt musi posiadać oznaczenie CE
Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta	Minimalny czas trwania gwarancji udzielonej przez producenta na monitor wynosi 60 miesięcy (5 lat).

4. Serwer

Minimalne wymagania podstawowe dla serwera z oprogramowaniem	
Parametr	**Charakterystyka (wymagania minimalne)**
Typ	Serwer z oprogramowaniem. W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego serwera.
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków wraz z kompletem teleskopowych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizerem do kabli. Na potrzeby przyszłej rozbudowy wymagana jest obudowa z możliwością wyposażania w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać 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	Na potrzeby przyszłej rozbudowy wymagana jest płyta główna z możliwością zainstalowania dwóch procesorów, wyposażona w minimum 16 slotów

Znak sprawy: GG.271.9.2022.WK

	przeznaczonych do instalacji pamięci, z możliwością obsługi 1TB pamięci RAM.
Procesor / wydajność	Serwer z zainstalowanym jednym procesorem 16-rdzeniowym, klasy x86 dedykowanym do pracy z zaoferowanym serwerem umożliwiający osiągnięcie w teście SPECrate®2017_int_base wyniku co najmniej 230 punktów przeprowadzonego dla konfiguracji dwuprocesorowej. Dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty raport z testu wydajności SPECrate®2017_int_base opublikowany na stronie www.spec.org dla oferowanego modelu serwera z oferowanym modelem procesora.
Pamięć operacyjna	Co najmniej 64GB RAM
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	Co najmniej jeden slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+, OCP 3.0
Dyski twarde	1) Serwer musi mieć możliwość instalacji dysków SAS, SATA, SSD 2) Zainstalowane 5 dysków SAS o pojemności min. 1.2TB, 12Gb, Hot-Plug. 3) Na potrzeby przyszłej rozbudowy musi zostać zapewniona możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. 4) Na potrzeby przyszłej rozbudowy musi zostać zapewniona możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego 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.
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 4GB nieulotnej pamięci cache, umożliwiający konfigurację co najmniej następujących poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wymagane wsparcie dla dysków SED.
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,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug o mocy max 600W.

Znak sprawy: GG.271.9.2022.WK

Bezpieczeństwo	▪ W celu ochrony przed nieautoryzowanym dostępem do dysków twardych wymagany jest zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz. ▪ Wymagany wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. ▪ Wymagany moduł TPM 2.0 pełniący funkcję dodatkowej warstwy sprzętowej do obsługi różnych działań kryptograficznych, w tym do ochrony kluczy szyfrowania, danych uwierzytelniania i innych wrażliwych danych.
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie komponentów serwera, w tym co najmniej: procesora, pamięci, dysków, BIOS'u, informacji o 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; ▪ 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; ▪ 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 i standardy	▪ Spełnianie postanowień normy ISO 9001 lub równoważnej w zakresie produkcji dla producenta sprzętu - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. ▪ Spełnienie postanowień normy ISO 14001 lub równoważnej w zakresie produkcji dla producenta sprzętu - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.

Znak sprawy: GG.271.9.2022.WK

	▪ Spełnienie postanowień normy ISO 50001 lub równoważnej dla produkcji serwerów przez producenta sprzętu - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. ▪ Oferowany serwer musi posiadać oznaczenie CE. ▪ Oferowany model serwera 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 gwarancyjno-serwisowe, wsparcie techniczne producenta	Serwer musi być objęty serwisem gwarancyjnym producenta przez min. 5 lat (60 miesięcy), z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Wymagana jest możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga gwarancji uwzględniającej zabezpieczenie serwisowe, które w przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, umożliwi pozostawienie uszkodzonego dysku u Zamawiającego (dysk nie będzie podlegał ekspertyzie poza siedzibą Zamawiającego) - przed podpisaniem umowy Zamawiający będzie żądał przedłożenia przez Wykonawcę oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku. Okres zabezpieczenia serwisowego na dyski twarde musi być zgodny z okresem udzielonej gwarancji na cały serwer. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń - dokumenty potwierdzające należy załączyć do oferty. Wymagana możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zaoferowane urządzenie musi mieć możliwość rozszerzenia gwarancji przez producenta do 7 lat.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Musi istnieć możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Znak sprawy: GG.271.9.2022.WK

System operacyjny	Oprogramowanie musi zostać dostarczone dla serwera fizycznego wyposażonego w 1 procesor wielordzeniowy. Jeśli dobór licencji zależy od liczby rdzeni procesora, Zamawiający ma obowiązek dostarczyć właściwą liczbę licencji dla liczby rdzeni procesora w oferowanym serwerze. Wraz z właściwą liczbą licencji na system operacyjny wymagane jest dostarczenie sumarycznie 20 licencji dostępowych na użytkownika współpracujących z dostarczanym systemem operacyjnym oraz nośnika CD/DVD zawierającego pakiet instalacyjny oferowanego systemu. Zamawiający wymaga dostarczenia licencji na oprogramowanie (system serwerowy) w najnowszej wersji obecnie dostępnej na rynku. Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

Znak sprawy: GG.271.9.2022.WK

	b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

	21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: ▪ Podłączenie 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. ▪ Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: ▪ Dystrybucję certyfikatów poprzez http ▪ Konsolidację CA dla wielu lasów domeny, ▪ Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, ▪ Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów.

	g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) budowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: ▪ 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 mode) 26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

Znak sprawy: GG.271.9.2022.WK

	29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

5. Serwer backupowy

Minimalne wymagania podstawowe dla serwera NAS (serwera backupowego)	
Parametr	**Charakterystyka**
Typ	Serwer typu NAS. W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego serwera.
Obudowa	Obudowa Rack o wysokości max 2U (wyposażona w elementy montażowe umożliwiające instalację urządzenia w szafie Rack), z możliwością instalacji min. 8 dysków wyposażona we wskaźniki diodowe sygnalizujące co najmniej następujące stany: zasilanie, status , stan każdego dysku, wskaźnik alarmu.
Pojemność dyskowa	8 zatok (kieszeni) z możliwością obsługi co najmniej dysków HDD SATA 2,5 i 3,5 cala o pojemności do 18TB dla każdego dysku. Musi być zapewniona możliwość rozbudowy (rozszerzenia) o 16 zatok
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
iSCSI	Wymagana obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Szyfrowanie	Wymagana możliwość szyfrowania folderów współdzielonych oraz całych woluminów kluczem AES 256 bitów. Wymagany mechanizm szyfrowania z akceleracją sprzętową.
Procesor	Procesor wielordzeniowy umożliwiający osiągnięcie w teście PassMark CPU Mark (Average CPU Mark) wyniku min. 1100 pkt. Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony www.cpubenchmark.net
Pamięć	RAM: min. 4GB z możliwością rozbudowy do 16GB. Flash: min. 512MB Masowa: min. 32GB - dyski dedykowane do pracy w urządzeniach NAS o parametrach nie gorszych niż złącze SATA III 6Gb/s, pamięć buforowa min. 64MB cache - wymagana liczba dysków 8 sztuk.
Interfejsy sieciowe	2x Port 2,5 Gigabit (2,5G/1G/100M), 2x 10 GbE SFP+
Porty	4x USB 3.2 Gen 1, 1 x PCIe Gen 2 x2
Obsługa trybów RAID	Wymagana możliwość pracy w trybie pojedynczy dysk, JBOD, RAID 0, 1, 5, 5+Spare, 6, 6+Spare, 10, 10+Spare, 50/60. Wymagana możliwość zwiększania pojemności i migracja między poziomami RAID online. Przywracanie RAID.

Znak sprawy: GG.271.9.2022.WK

Obsługiwane protokoły sieciowe	Co najmniej: CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Obsługiwane systemy plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ oraz exFAT
Usługi	Serwer pocztowy, Stacja monitoringu, Windows ACL, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Replikacja w czasie rzeczywistym, Klient LDAP, Serwer Syslog, Migawki wolumenów, Obsługa kontenerów (LXC – Docker), Serwer VPN
Pozostałe wymagania	Min. Liczba kont użytkowników: 4096 Min. Liczba grup: 512 Min. Liczba udziałów: 512 Max ilość połączeń: 700 Język GUI: Polski, Angielski
Zasilanie	▪ 100 - 240V, 50/60 Hz ▪ moc zasilaczy minimum 250W każdy ▪ Wymagana liczba zasilaczy: 2 ▪ Obsługa sieciowych awaryjnych zasilaczy UPS
Certyfikaty i standardy	Oferowany serwer musi posiadać oznaczenie CE
Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta	Serwer musi być objęty serwisem gwarancyjnym producenta przez min. 5 lat (60 miesięcy), z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Gwarancja na dyski co najmniej 3 lata (36 miesięcy).

6. Tworzenie domen platform portali tylko związane z cyberbezpieczenstwem i dostosowaniem do WCAG 2.1

Wymagania minimalne
Zamawiający Wymaga dostosowania strony internetowej Urzędu pod adresem https://www.gawluszowice.pl/ do standardu WCAG 2.1 oraz wymagań KRI. Zamawiający dopuszcza wykonanie strony internetowej na systemie Wordpress lub innym open source'owym systemie CMS. Zamawiający wymaga dostarczenia strony internetowej dostosowanej dla osób niepełnosprawnych (wymagana zmiana kontrastu, wielkości czcionki, skala szarości, podkreślenie linków, lupa, czarny kursor, podkreślenie tytułów, etykiety zdjęć, wyłączenie animacji) oraz strony responsywnej, która wyświetla się prawidłowo na urządzeniach mobilnych. Wymagane elementy składowe rozwiązania:

▪ Stroną główną całego rozwiązania będzie portal informacyjny. Ma on postać graficzną, prezentującą w sposób atrakcyjny wszystkie informacje serwisu. ▪ Strona powinna mieć mechanizmy: budowanie okienek pop-up, czat interaktywny (wielu operatorów obsługujących). ▪ Strona musi wyróżniać się wizualnym zarządzaniem zawartością treści, to znaczy, że zastosowane narzędzia muszą umożliwić zarządzanie zawartością poprzez przeciągnie bloków na stronie. Mechanizm zarządzania treścią prezentuje wizualnie na stronie treści i obrazy – tak jak widać je bez zalogowania. Administrator za pomocą urządzenia wskazującego na taki element/blok – może go przeciągnąć w dowolny inny obszar strony pomiędzy inne bloki, zawierające treści i obrazy. Zapisanie aktualizuje zawartość strony. ▪ Strona internetowa powinna automatycznie dostosowywać się do rozdzielczości monitora. ▪ Wykonawca przekaże instrukcje obsługi narzędzia. Wykonawca uwzględni, że instrukcja będzie skierowana do osób niemających specjalistycznej wiedzy informatycznej i będzie w języku polskim. ▪ Strona internetowa musi zapewniać bezpieczeństwo i poufność zgromadzonych dokumentów oraz danych przed nieautoryzowanymi zmianami. ▪ Komunikacja zalogowanych użytkowników ze Strony internetowej musi odbywać się wyłącznie za pomocą bezpiecznego połączenia szyfrowanego. Wymagania pozostałe: • Administrator zostanie przeszkolony w zakresie obsługi narzędzia. Szkolenie stacjonarne lub on-line do 6 godzin zegarowych.

7. Rozbudowa zabezpieczeń logicznych (firewall, IDS, IPS)

Minimalne wymagania podstawowe dla rozbudowy zabezpieczeń logicznych (firewall, IDS, IPS)	
Parametr	**Charakterystyka**
Typ	System firewall W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego systemu firewall oraz pełnej informacji o oferowanych serwisach o licencjach dostarczanych wraz z urządzeniem.
Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Zamawiający dopuszcza aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Znak sprawy: GG.271.9.2022.WK

	System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: ▪ Firewall. ▪ Ochrony w warstwie aplikacji. ▪ Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.

Znak sprawy: GG.271.9.2022.WK

	5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - minimum 600 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Zamawiający dopuszcza aby były one zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ▪ Translację jeden do jeden oraz jeden do wielu. ▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Znak sprawy: GG.271.9.2022.WK

	4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. ▪ Amazon Web Services (AWS). ▪ Microsoft Azure ▪ Google Cloud Platform (GCP). ▪ OpenStack. ▪ VMware NSX.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: ▪ Wsparcie dla IKE v1 oraz v2. ▪ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). ▪ Obsługa protokołu Diffie-Hellman grup 19 i 20. ▪ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. ▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. ▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. ▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. ▪ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. ▪ Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: ▪ Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. ▪ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. ▪ Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: ▪ Routingu statycznego. ▪ Policy Based Routingu.

Znak sprawy: GG.271.9.2022.WK

	▪ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

Znak sprawy: GG.271.9.2022.WK

	6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola www	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL. 5. Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: ▪ Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. ▪ Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

Znak sprawy: GG.271.9.2022.WK

	▪ Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

Znak sprawy: GG.271.9.2022.WK

	4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ▪ ICSA lub EAL4 dla funkcji Firewall.
Serwisy i licencje	W ramach realizacji zadania Zamawiający wymaga dostarczenia licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Zamawiający wymaga zapewnienia tej funkcjonalności przez okres jednego roku, w okresie realizacji projektu, tj. nie dłużej niż do 30.09.2023 r. Licencje powinny obejmować co najmniej: kontrolę aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.
Gwarancja	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.
Wymagania ogólne	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

VI. Instalacja i konfiguracja.

Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.	
Parametr	**Charakterystyka**

Wdrożenie	Celem prac jest przygotowanie systemu informatycznego (środowiska teleinformatycznego), na potrzeby realizacji projektu, zbudowanego w oparciu o dostarczone rozwiązania sprzętowe i oprogramowanie opisane w niniejszym dokumencie. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa. Po zapoznaniu się z architekturą sieciową urzędu Wykonawca przedstawi plan reorganizacji z uwzględnieniem istniejącego i dostarczanego sprzętu. Schemat ten musi być uzgodniony z Zamawiającym i uwzględniać jego wytyczne. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. **W ramach realizacji zamówienia Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych pod nadzorem Kierownika Projektu.** Zamawiający wymaga sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia. Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Dokumentacją Powykonawczą.
Montaż i fizyczne uruchomienie systemu	**Zamawiający wymaga zainstalowania dostarczonego sprzętu w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:** 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń (urządzenia sieciowe, urządzenia serwerowe) w szafie(-ach) rack w pomieszczeniu(-ach) (miejscach) wskazanych przez Zamawiającego . 2. Urządzenia, które nie są montowane w szafach teleinformatycznych np.: komputery, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 3. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 4. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 5. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.

Znak sprawy: GG.271.9.2022.WK

	6. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 7. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji - Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 8. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). 9. Demontaż „starych" urządzeń IT z szafy teleinformatycznej, które nie będą już wykorzystywane. 10. Po wykonaniu instalacji przeprowadzenie testów sprawdzających poprawność instalacji i działania urządzeń.
Konfiguracja elementów bezpieczeństwa sieciowego.	Urządzenie firewall Wykonawca skonfiguruje w następującym zakresie: 1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 2. Aktywacja (jeśli jest wymagana) urządzenia na stronie internetowej producenta. 3. Aktywacja (jeśli jest wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu gminy 5. Konfiguracja dostarczonego Firewall-a: a) Konfiguracja podstawowych parametrów b) Konfiguracja translacji adresów NAT c) Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, serwery komunikacyjne telefonii IP, itp. d) Konfiguracja inspekcji określonych protokołów sieciowych; e) Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall; f) Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; g) Testowanie działania bramy. 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS: a) Konfiguracja podstawowych parametrów; b) Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań; c) Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;

	d) Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; e) Testowanie działania ochrony IPS 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. a) Przypisanie adresu IP do zarządzania. b) Konfiguracja inspekcji protokołów HTTP, SMTP, FTP, POP3 c) Definicja reguł filtrowania/blokowania 8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej. 9. Uruchomienie i skonfigurowanie instancji systemu bezpieczeństwa dla skonfigurowanych sieci wirtualnych VLAN, taka liczba sieci wirtualnych aby odseparować różne typy ruchu, w porozumieniu z Zamawiającym. 10. W instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności: a) kontrola dostępu - zapora ogniowa klasy Statless Inspection b) ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar c) ochrona przed atakami - Intrusion Prevention System [IPS/IDS] d) kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. e) kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) f) kontrola pasma oraz ruchu [QoS, Traffic shaping] g) Kontrola aplikacji oraz rozpoznawanie ruchu P2P h) Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL) i) Inspekcja ruchu SSL j) Ochrony przez atakami na stacje klienckie k) Kontrola pasma 11. Konfiguracja logowania i raportowania. 12. Konfiguracja logowania i raportowania do alternatywnego serwera SYSLOG uruchomionego na serwerze NAS (instalacja i konfiguracja serwera SYSLOG spoczywa na Wykonawcy). Jeśli dla zapewnienia tej funkcjonalności wymagane są jakiekolwiek licencje - ich dostarczenie spoczywa na Wykonawcy.

Znak sprawy: GG.271.9.2022.WK

Instalacja i konfiguracja serwera, instalacja systemu operacyjnego serwera	Zamawiający wymaga wykonania fizycznej instalacji serwera we wskazanej szafie Rack oraz: 1. Przygotowania konfiguracji odpowiedniego poziomu RAID wskazaną przez Zamawiającego. 2. Instalacji systemów operacyjnych oraz ich aktywacji 3. Instalacji niezbędnych aktualizacji oraz poprawek związane z bezpieczeństwem udostępnionych przez producenta systemu operacyjnego.
Uruchomienie usługi katalogowej oraz niezbędnych komponentów, migracja danych do/z obecnej usługi katalogowej	Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na serwerze wraz z komponentami odpowiedzialnymi za rozwiązywanie nazw. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowany system operacyjny, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem. Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego. Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi: a) Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości b) Śledzenie zmian dotyczących tworzenia, usuwania obiektów Zamawiający wymaga skonfigurowania jednej stacji zarządzającej. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).
Konfiguracja polityki haseł oraz polityki blokowania kont	Konfiguracja globalnej polityki haseł dla domeny: a) Hasło musi zawierać minimum 8 znaków b) Maksymalny czas ważności hasła: do ustalenia z Zamawiającym c) Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym d) Hasło musi spełniać zasady złożoności Konfiguracja polityki haseł dla kadry zarządzającej: a) Hasło musi zawierać minimum 10 znaków b) Maksymalny czas ważności hasła: 30 dni c) Minimalny czas, po którym możliwa jest zmiana hasła: 30 dni d) Hasło musi spełniać zasady złożoności

Znak sprawy: GG.271.9.2022.WK

	Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach. Szczegółowe dane zostaną przekazane na etapie konfiguracji.
Dołączenie stacji roboczych do domeny	Zamawiający wymaga przygotowania schematu, dołączenia dostarczonych stacji roboczych do domeny oraz przeszkolenie wyznaczonego pracownika. W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mających na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (między innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na konto domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji).
Uruchomienie i skonfigurowanie serwera NAS	Zamawiający wymaga uruchomienia oraz skonfigurowanie serwera plików NAS dedykowanego na kopie zapasowe.
Uruchomienie i konfiguracja systemu zarządzania kopiami zapasowymi	1. Instalacja oprogramowania do wykonywania kopii zapasowych. 2. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania: a) kopie muszą być wykonywane na serwer NAS; b) kopie muszą być wykonywane automatycznie wg zadanego harmonogramu; c) kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową; d) musi istnieć możliwość odtworzenia: ▪ całego systemu; ▪ dysku serwera; ▪ pojedynczych plików serwera 3. Zdefiniowanie powiadomień o przebiegu wykonania kopii i zdarzeniach. 4. Uruchomienie testowych zadań backupu. 5. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email. 6. Uruchomienie testowych zadań odtworzenia danych. 7. Przeszkolenie pracowników w zakresie obsługi systemu do wykonywania kopii zapasowych, wykonywania kopii zapasowych oraz odtwarzania danych.
Migracja systemów	Zamawiający wymaga instalacji, konfiguracji oraz przeniesienia wykorzystywanego oprogramowania i bazy danych wykorzystywanych w

	placówce na nowy serwer. Po wykonaniu migracji zostaną przeprowadzone testy sprawdzające poprawność wykonania czynności.
Wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą.
Opracowanie dokumentacji powykonawczej	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej).
Szkolenie dla administratora	Wykonawca w okresie wdrożenia przeprowadzi w siedzibie Zamawiającego szkolenia dla Administratora systemu, łącznie w wymiarze min. 6 godzin szkolenia. Szkoleniem zostaną objęte osoby wskazane przez Zamawiającego z zakresie dostarczonego rozwiązania teleinformatycznego, co najmniej w zakresie: ▪ Dostarczonego sprzętu. ▪ Dostarczonego oprogramowania (systemu operacyjnego). ▪ Systemu backupu. Celem szkolenia administratora będzie zapoznanie się z systemem informatycznym, poznanie poszczególnych funkcji i modułów oraz nauka jego obsługi w praktyce. Na etapie wdrożenia strony ustalą szczegółowy porządek i podział szkoleń z uwzględnieniem wymagań zawartych w niniejszym rozdziale, które przyjęte zostaną w planie szkoleń. Wykonawca zobowiązany jest do przeprowadzenia szkoleń w formie instruktażu stanowiskowego dla personelu w podziale na role w Systemie. Taki sposób przeprowadzenia szkoleń jest najbardziej efektywny i umożliwi personelowi rozpoczęcie pracy zaraz po zakończeniu szkolenia.

VII. DIAGNOZA CYBERBEZPIECZEŃSTWA

Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina", opisanymi na stronie https://www.gov.pl/web/cppc/cyfrowa-gmina

Wykonawca musi wykonać usługę zgodnie zakresem oraz z formularzem stanowiącym załącznik do dokumentacji konkursowej. załączniku nr Załącznik_nr_8_-_Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa

Znak sprawy: GG.271.9.2022.WK

Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Zamawiający nie dopuszcza wykonania diagnozy cyberbezpieczeństwa w sposób zdalny - wykonawca podejmujący się realizacji diagnozy zobowiązany jest do jej przeprowadzania w miejscu świadczenia usługi w siedzibie Zamawiającego. Diagnoza musi zostać przeprowadzona w maksymalnym stopniu obiektywnie - poprzez przeprowadzone badanie w Urzędzie Gminy w celu przedstawienia rzeczywistego stanu cyberbezpieczeństwa Urzędu. Zamawiający zakłada, że Wykonawca przeznaczy nie więcej niż 3 dni na wykonanie diagnozy (audytu) z tego minimum 1 dzień spędzi w Urzędzie Gminy na prowadzenie analiz do audytu w kontakcie z wskazanymi przez Zamawiającego pracownikami urzędu.