Załącznik nr 2 do SWZ

Szczegółowy Opis Przedmiotu Zamówienia

Dostawa sprzętu komputerowego, oprogramowania informatycznego oraz usług szkoleniowo-audytowych w ramach realizacji projektu grantowego „Cyfrowa Gmina"

Część I: Zakup, dostawa i wdrożenie sprzętu komputerowego, sprzętu informatycznego i oprogramowania dla Urzędu Miasta i Gminy Chmielnik w ramach projektu „Cyfrowa Gmina"

1. Dostawa, instalacja i uruchomienie sprzętu

Mając na uwadze nadrzędność celu jakim jest skuteczne uruchomienie planowanych rozwiązań Zamawiający zastrzega, że zadaniem Wykonawcy jest dostarczenie wszelkich niezbędnych elementów sprzętowych, oprogramowania, licencji oraz wykonanie wszystkich niezbędnych prac instalacyjnych, konfiguracyjnych i wdrożeniowych, które konieczne są do prawidłowego działania zgodnie z przeznaczeniem, nawet jeśli nie zostały one wymienione w dalszej części niniejszego dokumentu.

1.1.Wymagania ogólne

W ramach przedmiotowego zamówienia, Zamawiający wymaga dostarczenia, instalacji oraz konfiguracji sprzętu i oprogramowania systemowego oraz bazodanowego, którego parametry minimalne zostały wskazane poniżej. Zamawiający akceptuje sprzęt oraz oprogramowanie o wyższych (lepszych) parametrach użytkowych lub wykonany w nowszej technologii pod warunkiem, że produkty zaoferowane przez Wykonawcę spełniają wszystkie parametry minimalne.

Wszystkie oferowane przez Wykonawcę produkty muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta, posiadać wszystkie wymagane certyfikaty i oznaczenia oraz spełniać wszystkie wymagane prawem normy.

Zamawiający wymaga, by dostarczone urządzenia były nowe (wyprodukowane nie wcześniej, niż na 6 miesięcy przed ich dostarczeniem) oraz aby nie były używane.

Zamawiający wymaga kompleksowego uruchomienia i zainstalowania dostarczonego sprzętu oraz oprogramowania.

a) Oprogramowanie systemowe

Dostarczone systemy operacyjne oraz wszystkie niezbędne oprogramowanie dodatkowe na serwerach ma być kompletnie zainstalowane, spersonalizowane oraz aktywowane o ile jest to wymagane.

Konfiguracja logiczna sprzętu (nazwy sieciowe, adresy IP, nazwy i konta użytkowników) ma być przeprowadzona zgodnie z zaleceniami Zamawiającego.

W ramach dostarczenia serwerowych systemów operacyjnych Zamawiający wymaga uruchomienia i wdrożenia w siedzibie zamawiającego funkcjonalności Active Directory wraz

z utworzeniem kont dla wszystkich użytkowników oraz przeniesieniem danych każdego użytkownika.

b) Sprzęt

Zamawiający wymaga, aby wszystkie dostarczone urządzenia zostały umieszczone (zamontowane) i uruchomione we wskazanych przez Zamawiającego miejscach przeznaczenia, w uzgodnionym przez obie strony terminie. Sposób montażu sprzętu ma być dostosowany do technologii wykonania oraz ma być przeprowadzony zgodnie z zaleceniami producenta. Wykonawca dostarczy wszystkie niezbędne kable połączeniowe pomiędzy serwerami, dyskiem sieciowym oraz przełącznikiem, zapewniające transmisję danych z pełną prędkością łączonych portów.

Wykonawca musi zapewnić asystę 30 godzin do wykorzystania maksymalnie do 6 miesięcy od momentu dostarczenia sprzętu i oprogramowania.

Ogólne zasady równoważności rozwiązań

W celu zachowania neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za równoważne rozwiązanie uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp. a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny sposób, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Wykonawca odpowiedzialny jest za dostawę w pełni funkcjonujących rozwiązań opisanych w niniejszym załączniku, w tym jeżeli jest konieczne, pozyskanie niezbędnych informacji do realizacji zamówienia, zawarcie koniecznych umów itp.

1.2.Serwer aplikacyjny – 1 szt.

Element konfiguracji	Wymagane minimalne parametry techniczne
Obudowa	Obudowa typu RACK maksymalnie 1U, przystosowana do montażu w szafie 19” wraz z szynami montażowymi
Procesor	Zainstalowany minimalnie 1 procesor, maksymalnie 16-rdzeniowy, w architekturze x86 – 64 bity, osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 150 punktów dla oferowanej konfiguracji. Wynik testu musi być opublikowany na stronie http://spec.org w dniu złożenia oferty
Płyta główna	Płyta główna zaprojektowana do pracy w serwerach z minimum 16 slotami na pamięć i umożliwiająca instalację do minimum 1TB pamięci. Płyta główna z fabrycznym oznaczeniem logo producenta (dopuszcza się logo producenta na module zarządzania trwale zintegrowanym na płycie głównej).
Pamięć operacyjna	Minimum 64 GB pamięci RAM typu DDR4 3200 MHz w modułach o pojemnościach 32 GB każdy.
Sloty rozszerzeń	Serwer musi być wyposażony w: - 2 aktywne gniazda PCI-Express generacji 4 gotowe do obsadzenia kartami sieciowymi, każde gniazdox16 (szybkość slotu – bus width) serwer musi mieć dodatkowo dedykowane min dwa sloty PCI-Express: - jeden na kontroler dyskowy, Drugi na kartę sieciową 10/25 GB Ethernet dwuportową.
Pamięć masowa	Zatoki dyskowe gotowe do zainstalowania 8 dysków typu Hot Swap, SAS/SATA/SSD 2,5” Zainstalowane 4 dyski Hot Swap 1,2 TB SAS 12 G 10k. Zainstalowane 2 dyski SSD NVME o pojemności 480 GB sprzętowo zabezpieczone RAID-1 ze wsparciem dla oprogramowania VMware
Kontroler	Kontroler sprzętowy, nie zajmujący slotu PCIe, mogący pracować jako HBA lub kontroler RADI, zapewniający obsługę do 16 napędów dyskowych SAS/SATA oraz obsługujący poziomy:

	RAID0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem zawartości na wypadek awarii zasilania. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
Interfejsy sieciowe	Serwer musi być wyposażony minimum w 4 porty 1 Gb RJ-45
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Porty	2xUSB 3.0 lub nowsze 1xVGA Możliwość rozbudowy o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy, bez pośrednictwa portu USB/RJ-45. Nie dopuszcza się stosowania kart PCI.
Zasilacz	2 szt. Typu Hot-plug, redundantne, każdy o mocy minimum 500W
Chłodzenie	Zestaw wentylatorów zapewniających wydajne chłodzenie serwera
Karta/moduł zarządzający i system zarządzania	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Expres, jednak nie może ona powodować zmniejszenia minimalnej wymaganej liczby gniazd PCI Express w serwerze, posiadająca minimalną funkcjonalność: - monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe - możliwość pracy w trybie bez agentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP - dostęp do karty zarządzającej poprzez * dedykowany port RJ-45 z tyłu serwera lub * przez współdzielony port zintegrowanej karty sieciowej serwera. - dostęp do karty możliwy: z poziomu przeglądarki webowej (GUI), z poziomu linii komend

	- wirtualna zdalna kontrola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB oraz wirtualnych folderów - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) - zdalna aktualizacja oprogramowania (frimware) - wsparcie dla Microsoft Active Directory - wsparcie dla IPv4 oraz IPv6, obsługa SNMPv3 oraz RESTful API, Możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) Dodatkowo wymagane jest dostarczenie centralnego systemu do zarządzania serwerami w ramach tego postępowania. Dopuszcza się system w formie wiryualnej maszyny, dla której Zamawiający udostępni odpowiednie zasoby w swoim środowisku wirtualnym. System zarządzania musi zapewniać: - zdalne włączenie/wyłączenie/ restart niezależnie dla każdego serwera - przedstawienie graficznej reprezentacji w formie 3D temperatury w serwerowni z możliwością identyfikacji najgorętszych miejsc do poziomu szafy technicznej lub serwera - wizualizację wykorzystania procesorów (CPU), poboru energii przez serwer i temperatury w czasie rzeczywistym. Wymagana możliwość rysowania widoku centrum przetwarzania danych i nanoszenia na niego serwerów i szaf stelażowych - bez agentowe zarządzanie i monitorowanie stanu urządzeń -pojedynczy interfejs zapewniający widoki, podsumowanie szczegółowych informacji o sprzęcie i oprogramowaniu układowym zainstalowanym na serwerach - udostępnienie przez interfejs REST API oraz interfejs graficzny użytkownika - Zarządzanie uprawnieniami użytkowników poprzez definiowanie ról

	- Konfigurację środowiska serweró1.3. stelażowych w oparciu o logiczne profile serwerowe. W zakresie logicznego profilu serwera muszą wchodzić następujące parametry: * sekwencja bootowania systemu, ustawienia BIOS, wersja oprogramowania układowego i sterowników (dla Windows, Vmware i Red Hat) * Ustawienia BIOS pozwalające na minimum: włączenie/wyłączenie funkcji hiper threading w procesorach Intel, włączenie/wyłączenie rdzeni procesora, włączenie/wyłączenie funkcji wirtualnych, zmiana ustawień poziomu poboru prądu, ustawienia trybu turbo boost w procesorach Intel, ustawienia trybu zabezpieczenia pamięci RAM * Konfiguracja dysków lokalnych * Konfiguracja użytkowników karty/modułu zarządzania serwerem - monitorowanie utylizacji serwera: procesorów, zasilania, temperatury, - integrację z narzędziami takimi jak Vmware vCenter oraz Microsoft System Center przez specjalną wtyczkę (np. dodatkowe zakładki) w tych aplikacjach, rozszerzającą możliwości zarządzania o warstwę sprzętową
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Windows Server 2016 Windows Server 2019 (Most Recent Version) Windows Server 2022 VMware ESXi 6.7 U3 VMware ESXi 7.0 U1/U2 SUSE Linux Enterprise Server (SLES)12 SP5 SUSE Linux Enterprise Server (SLES)15 SP2 Red Hat Enterprise Linux (RHEL) 8.3 Citrix Hypervisor 8,2 Ubuntu 20.04 LTS
Wsparcie techniczne	3 letnia gwarancja producenta w miejscu instalacji

	2-godzinny czas reakcji w godzinach od 9:00 do 17:00 (standardowe dni robocze). Przybycie na miejsce w następnym dniu roboczym. Wsparcie techniczne realizowane jest przez organizację serwisową producenta oferowanego serwera. Obsługa prowadzona w języku polskim.
Certyfikaty i standardy	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja Zgodności CE.
System operacyjny	Oprogramowanie Windows Serwer Standard 2022 lub system równoważny. Zamawiający wymaga dostarczenia licencji na Windows Serwer Standard w ilości zapewniającej uruchomienie minimum 4 maszyn wirtualnych na dostarczonym serwerze oraz pokrycie na oferowaną sumaryczną liczbę rdzeni lub system równoważny obsługujący technologię COM, .NET posiadający możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory opartej o Windows Serwer* i w pełni wspierające MS Exchange*, MS System Center Configuration Manager*, MS Lync* oraz umożliwiający implementację min. 2 szt. Maszyn wirtualnych opartych o usługę Hyper-V na każdą zaoferowaną licencję. Licencje dostępowe do Windows Serwer Zamawiający wymaga dostawy minimum 55 licencji dostępowych do oferowanych licencji serwera licencjonowanych na użytkownika.
Oprogramowanie wirtualizacji	1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych 2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.

	3. Pojedynczy klaster może się składać do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. 4. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB. 5. Oprogramowanie do wirtualizacji musi zapewniać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM. 6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. 7. Oprogramowanie do wirtualizacji musi zapewniać możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. 8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB. 9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej. 10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10, Windows Server, Amazon Linux2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, Core OS, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Phyton OS. 13. Rozwiązane musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. 14. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instalacji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.

	16. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. 17. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączenia do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. 18. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN) 19. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. 20. Rozwiązanie musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora. 21. Oprogramowanie do wirtualizacji musi zapewniać możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 22. Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. 23. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wistualnej. 24. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej maszyny wirtualnej tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5. 25. Rozwiązanie musi zapewniać możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów,

	pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne. 26. Wsparcie 3 lata.

1.3. Serwer kopii zapasowych – 1 szt.

Element konfiguracji	Wymagane minimalne parametry techniczne
Obudowa	Obudowa typu RACK maksymalnie 1U, przystosowana do montażu w szafie 19” wraz z szynami montażowymi
Procesor	Zainstalowany minimalnie 1 procesor, maksymalnie 16-rdzeniowy, w architekturze x86 – 64 bity, osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 150 punktów dla oferowanej konfiguracji. Wynik testu musi być opublikowany na stronie http://spec.org w dniu złożenia oferty
Płyta główna	Płyta główna zaprojektowana do pracy w serwerach z minimum 16 slotami na pamięć i umożliwiająca instalację do minimum 1TB pamięci. Płyta główna z fabrycznym oznaczeniem logo producenta (dopuszcza się logo producenta na module zarządzania trwale zintegrowanym na płycie głównej).
Pamięć operacyjna	Minimum 64 GB pamięci RAM typu DDR4 3200 MHz w modułach o pojemnościach 32 GB każdy.
Sloty rozszerzeń	Serwer musi być wyposażony w: - 2 aktywne gniazda PCI-Express generacji 4 gotowe do obsadzenia kartami sieciowymi, każde gniazdox16 (szybkość slotu – bus width) serwer musi mieć dodatkowo dedykowane min dwa sloty PCI-Express: - jeden na kontroler dyskowy, Drugi na kartę sieciową 10/25 GB Ethernet dwuportową.
Pamięć masowa	Zatoki dyskowe gotowe do zainstalowania 8 dysków typu Hot Swap, SAS/SATA/SSD 2,5” Zainstalowane 4 dyski Hot Swap 1,2 TB SAS 12 G 10k. Zainstalowane 2 dyski SSD NVME o pojemności 480 GB sprzętowo zabezpieczone RAID-1 ze wsparciem dla oprogramowania VMware

Kontroler	Kontroler sprzętowy, nie zajmujący slotu PCIe, mogący pracować jako HBA lub kontroler RADI, zapewniający obsługę do 16 napędów dyskowych SAS/SATA oraz obsługujący poziomy: RAID0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem zawartości na wypadek awarii zasilania. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
Interfejsy sieciowe	Serwer musi być wyposażony minimum w 4 porty 1 Gb RJ-45
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Porty	2xUSB 3.0 lub nowsze 1xVGA Możliwość rozbudowy o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy, bez pośrednictwa portu USB/RJ-45. Nie dopuszcza się stosowania kart PCI.
Zasilacz	2 szt. Typu Hot-plug, redundantne, każdy o mocy minimum 500W
Chłodzenie	Zestaw wentylatorów zapewniających wydajne chłodzenie serwera
Karta/moduł zarządzający i system zarządzania	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Expres, jednak nie może ona powodować zmniejszenia minimalnej wymaganej liczby gniazd PCI Express w serwerze, posiadająca minimalną funkcjonalność: - monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe - możliwość pracy w trybie bez agentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP - dostęp do karty zarządzającej poprzez * dedykowany port RJ-45 z tyłu serwera lub * przez współdzielony port zintegrowanej karty sieciowej serwera. - dostęp do karty możliwy: z poziomu przeglądarki webowej (GUI), z poziomu linii komend

	- wirtualna zdalna kontrola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB oraz wirtualnych folderów - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) - zdalna aktualizacja oprogramowania (frimware) - wsparcie dla Microsoft Active Directory - wsparcie dla IPv4 oraz IPv6, obsługa SNMPv3 oraz RESTful API, Możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) Dodatkowo wymagane jest dostarczenie centralnego systemu do zarządzania serwerami w ramach tego postępowania. Dopuszcza się system w formie wiryualnej maszyny, dla której Zamawiający udostępni odpowiednie zasoby w swoim środowisku wirtualnym. System zarządzania musi zapewniać: - zdalne włączenie/wyłączenie/ restart niezależnie dla każdego serwera - przedstawienie graficznej reprezentacji w formie 3D temperatury w serwerowni z możliwością identyfikacji najgorętszych miejsc do poziomu szafy technicznej lub serwera - wizualizację wykorzystania procesorów (CPU), poboru energii przez serwer i temperatury w czasie rzeczywistym. Wymagana możliwość rysowania widoku centrum przetwarzania danych i nanoszenia na niego serwerów i szaf stelażowych - bez agentowe zarządzanie i monitorowanie stanu urządzeń -pojedynczy interfejs zapewniający widoki, podsumowanie szczegółowych informacji o sprzęcie i oprogramowaniu układowym zainstalowanym na serwerach - udostępnienie przez interfejs REST API oraz interfejs graficzny użytkownika - Zarządzanie uprawnieniami użytkowników poprzez definiowanie ról

	- Konfigurację środowiska serweró1.4. stelażowych w oparciu o logiczne profile serwerowe. W zakresie logicznego profilu serwera muszą wchodzić następujące parametry: * sekwencja bootowania systemu, ustawienia BIOS, wersja oprogramowania układowego i sterowników (dla Windows, Vmware i Red Hat) * Ustawienia BIOS pozwalające na minimum: włączenie/wyłączenie funkcji hiper threading w procesorach Intel, włączenie/wyłączenie rdzeni procesora, włączenie/wyłączenie funkcji wirtualnych, zmiana ustawień poziomu poboru prądu, ustawienia trybu turbo boost w procesorach Intel, ustawienia trybu zabezpieczenia pamięci RAM * Konfiguracja dysków lokalnych * Konfiguracja użytkowników karty/modułu zarządzania serwerem - monitorowanie utylizacji serwera: procesorów, zasilania, temperatury, - integrację z narzędziami takimi jak Vmware vCenter oraz Microsoft System Center przez specjalną wtyczkę (np. dodatkowe zakładki) w tych aplikacjach, rozszerzającą możliwości zarządzania o warstwę sprzętową
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Windows Server 2016 Windows Server 2019 (Most Recent Version) Windows Server 2022 VMware ESXi 6.7 U3 VMware ESXi 7.0 U1/U2 SUSE Linux Enterprise Server (SLES)12 SP5 SUSE Linux Enterprise Server (SLES)15 SP2 Red Hat Enterprise Linux (RHEL) 8.3 Citrix Hypervisor 8,2 Ubuntu 20.04 LTS
Wsparcie techniczne	3 letnia gwarancja producenta w miejscu instalacji 2-godzinny czas reakcji w godzinach od 9:00 do 17:00 (standardowe dni robocze). Przybycie na miejsce w następnym dniu roboczym.

	Wsparcie techniczne realizowane jest przez organizację serwisową producenta oferowanego serwera. Obsługa prowadzona w języku polskim.
Certyfikaty i standardy	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja Zgodności CE.
System operacyjny	Oprogramowanie Windows Serwer Standard 2022 lub system równoważny. Zamawiający wymaga dostarczenia licencji na Windows Serwer Standard w ilości zapewniającej uruchomienie minimum 4 maszyn wirtualnych na dostarczonym serwerze oraz pokrycie na oferowaną sumaryczną liczbę rdzeni lub system równoważny obsługujący technologię COM, .NET posiadający możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory opartej o Windows Serwer* i w pełni wspierające MS Exchange*, MS System Center Configuration Manager*, MS Lync* oraz umożliwiający implementację min. 2 szt. Maszyn wirtualnych opartych o usługę Hyper-V na każdą zaoferowaną licencję.

1.5. Komputer stacjonarny – 20 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Komputer	Komputer będzie wykorzystywany na potrzeby aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu.
Obudowa	Typu mini tower z obsługą kart PCI Express o wysokim profilu. Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. na napęd optyczny (dopuszcza się stosowanie napędów slim)zewnętrzna, 1 szt. na standardowy dysk twardy 3,5” lub na dysk M.2

	- Wbudowany czujnik otwarcia obudowy, - Wbudowany głośnik min. 2W - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, PN, numerem seryjnym
Zasilacz	Maksymalnie 180 W o sprawności minimum 85%
Chipset	Dostosowany do zaoferowanego procesora
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera. Wyposażona w złącza min.: - 1xPCI Express 3.0x16 - 1xPCI Express 3.0x1 - 2xM.2 z czego min. Jedna przeznaczona dla dysku SSD z obsługą PCIe NVMe
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach równej lub wyższej 16000 punktów na podstawie PassMark PerformanceTest w teście CPU Mark według wyników Average CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. (Do oferty należy załączyć wydruk z przeprowadzonych testów na konfiguracji identycznej z zaoferowaną lub link do strony producenta testu z opublikowanym wynikiem).
Pamięć operacyjna	Minimum 8 GB DDR4 z możliwością rozszerzenia do 64 GB Ilość banków pamięci min. 2 szt. Ilość wolnych banków pamięci min. 1 szt.
Dysk twardy	Minimum 256 SSD PCIe NVMe, zawierający partycję Recovery umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii
Napęd optyczny	Nagrywarka DVD+/- RW
Karta graficzna	Zintegrowana karta graficzna
Dźwięk	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition
Karta sieciowa	LAN 10/100/1000 Mbit/s z funkcją PXE oraz Wake on LANWbudowana karta WiFi AC+BT 5.0
Porty/złącza	Wbudowane porty/złącza:

	Wideo umożliwiające podłączenie urządzenia bez stosowania przejściówek lub adapterów za pomocą min: - 1 x VGA, - 1 x HDMI, - 1 x DisplayPort Pozostałe porty/złącza: - minimum 8 x USB (w tym min. 4 szt. z przodu obudowy z czego min. 2 x USB 3.2 oraz min. 4 x USB z tyłu obudowy) - Port sieciowy Rj-45 - Port COM - Port słuchawek i mikrofonu na przednim panelu lub tylnym panelu obudowy - Port line-in na tylnym panelu - czytnik kart multimedialnych wbudowany w obudowę, Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp.
Klawiatura/mysz	Klawiatura przewodowa w układzie US z wydzielonym blokiem klawiszy numerycznych. Mysz przewodowa (scroll).
System operacyjny	System operacyjny Windows 10 lub 11 Pro 64-bit lub równoważny klasy PC. Musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.

	5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.

	19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.

	32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Oprogramowanie biurowe	Oprogramowanie biurowe z licencją wieczystą zawierające minimum: •arkusz kalkulacyjny, •edytor tekstu, •program do tworzenia prezentacji,

	Programy wchodzące w skład pakietu muszą w 100% odwzorowywać treść i układ dokumentów doc, docx, rtf, xls, xlsx, ppt, pptx wytworzonych w posiadanych przez Zamawiającego pakietach Microsoft Office od wersji 2013 Edytor tekstu musi poprawnie odwzorowywać wszystkie elementy umieszczone w nagłówkach i stopkach dokumentów DOC oraz DOCX, obsługiwać osadzanie innych dokumentów tekstowych oraz arkuszy kalkulacyjnych. Dla wstawianych obiektów typu „wykres" musi istnieć możliwość osadzenia danych służących do utworzenia tego wykresu z możliwością ich edycji bezpośrednio z edytora tekstu lub poprzez otwarcie danych w dostarczanym arkuszu kalkulacyjnym. Edycja 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. Śledzenie zmian wprowadzonych przez użytkowników. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Arkusz kalkulacyjny musi umożliwiać użycie wszystkich funkcji dostępnych w posiadanym przez Zamawiającego oprogramowaniu Microsoft Excel od wersji 2013. Arkusz kalkulacyjny musi zawierać (lub umożliwiać doinstalowanie bezpłatnego dodatku) oprogramowanie umożliwiające zoptymalizować wartość komórek zmienianych w celu uzyskania oczekiwanego rezultatu końcowego, przy jednoczesnym spełnieniu wszystkich zdefiniowanych parametrów oraz ograniczeń. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe ora formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową analizę wariantową i rozwiązywanie problemów optymalizacyjnych. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynność. Formatowanie czasu, daty i wartości finansowych z polskim formatem. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

	Program do prezentacji musi poprawnie obsługiwać wszystkie animacje i przejścia utworzone w posiadanym przez Zamawiającego programie Microsoft Power Point od wersji 2013. Program musi umożliwiać prezentowanie przy użyciu projektora multimedialnego. Drukowanie w formacie umożliwiającym robienie notatek. Zapisanie jako prezentacja tylko do odczytu, nagrywanie narracji i dołączanie jej do prezentacji, opatrywanie slajdów notatkami dla prezentera. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, tabel i wykresów pochodzących z arkusza kalkulacyjnego. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. Możliwość tworzenia animacji obiektów i całych slajdów. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym, monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
BIOS	BIOS zgodny ze specyfikacją UEFI. Musi umożliwiać, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych, odczyt informacji o: - modelu komputera, - numerze seryjnym, - MAC adres karty sieciowej, - wersja BIOS wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku i napędu optycznego) Możliwość z poziomu BIOS: - wyłączania/włączania portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB,

	2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej, - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora, - załadowania optymalnych ustawień BIOS, - obsługa BIOS za pomocą klawiatury i myszy.
Zintegrowany system diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego lub SSD • test monitora • Testy magisterskie PCI-e • test portów USB • test płyty głównej • test myszy i klawiatury • test procesora Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • Komputer PC: producent, model • BIOS: wersja oraz data wydania • Procesor: nazwa, taktowanie • Pamięć RAM: ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci Dysk: model, numer seryjny, wersja firmware, pojemność, temperatura pracy
Certyfikaty i standardy	- Certyfikat ISO 9001:2015 dla producenta sprzętu (należy załączyć do oferty) - TCO Certified Desktops 8 (ceryfikat musi znajdować się na stronie organizacji) - Deklaracja zgodności CE (załączyć do oferty) - Zgodność z dyrektywą RoHS Unii Europejskiej

	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie bezczynności (IDLE) wynosząca maksymalnie 25 dB
Rozmiary urządzenia	Wysokość nie może być większa niż 35 cm Szerokość nie może być większa niż 15 cm
Bezpieczeństwo	- Moduł TPM 2.0 - Złącze typu Kensington Lock, - Czujnik otwarcia obudowy.
Gwarancja	Gwarancja producenta świadczona w miejscu użytkowania sprzętu (Onsite). Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
Wsparcie techniczne producenta	▪ Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera ▪ Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie Producentowi), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. ▪ Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera ▪ Infolinia wsparcia technicznego dostępna w dni powszednie od 9:00-18:00 – możliwość kontaktu przez telefon, formularz web lub chat online, ▪ Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.

1.6. Monitor – 20 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Monitor	Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, obróbki zdjęć lub wideo. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację monitora
Wielkość ekranu	Przekątna ekranu min. 23,8”
Matryca	Typu IPS/PLS/UWVA o wykończeniu matowym (nie dopuszcza się naklejek matowiących matrycę)
Czas reakcji	Maks. 6 ms
Rozdzielczość i wielkość piksela	Rozdzielczość nie mniejsza niż: FHD (1920x1080) Piksel nie większy niż – 0.28 mm
Kąty widzenia	Kąty widzenia min. 178 stopni w pionie i w poziomie
	Nie mniejszy niż 70% NTSC
Kontrast i jasność	Kontrast nie mniejszy niż: 1000:1 Jasność nie mniejsza niż 250 cd/m2
Porty/złącza	Minimalna ilość dostępnych złącz monitora: – 1x DP – 1x ZŁĄCZE HDMI – 1 gniazdo VGA
Głośniki	Min. 2x 1.5W
Kable	Wymagane kable w zestawie z monitorem min.: – Złącze HDMI – Kabel zasilający
Podstawa monitora	Musi umożliwiać: – przechylenie w pionie – regulację wysokości – pivot – obrót wokół osi (swivel)
Obudowa	– musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona)

	– Możliwość zainstalowania monitora na ścianie przy wykorzystaniu ściennego systemu montażowego VESA (100x100) – Wbudowane w obudowę przyciski umożliwiające włączenie, wyłączenie oraz zmianę ustawień wyświetlania monitora – Obudowa trwale oznaczona numerem seryjnym i katalogowym pozwalającym na jednoznaczna identyfikacje zaoferowanego monitora – Wbudowany zasilacz w obudowie
Certyfikaty i standardy	- Certyfikat EPEAT na poziomie co najmniej Silver, - TCO 8.0, - TCO Edge, - Gwiazda Energii.
Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji Możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego.

1.7. Dysk sieciowy NAS – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Minimum 4 rdzeniowy, 32 bitowy o taktowaniu nie mniejszym niż 1,7 GHz
Pamięć RAM	Nie mniej niż 8GB SODIMM DDR3 z możliwością rozbudowy do 16 GB
Pamięć Flash	Nie mniej niż 512 MB
Liczba zatok na dyski twarde	Minimum 4
Obsługiwane dyski twarde	3,5” oraz 2,5” SATA oraz 2,5” SSD SATA
Pojemność dysków twardych	do 16 TB
Porty LAN 1 GB/s	Minimum 2 RJ-45
Porty LAN 10GB/s	Minimum 1 SFP+

Porty USB 3.0	Minimum 4
Obudowa	RACK wraz z szynami do montażu w szafie
Zasilanie	Zasilacz o mocy min 100 W
Przyciski	Reset, Zasilanie
Diody Led	Status, LAN, HDD, USB
Oprogramowanie	
Agregacja łączy	tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Łączenie usług z interfejsem	Tak
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	- Pojedynczy dysk, RAID 0,1,5,6,10, 5+ 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 - Globalny Hot Spare, - Pula pamięci masowej
Wbudowana obsługa iSCSI	- Multi-LUNs na Target, - Obsługa lun Mapping&Masking - Obsługa SPC-3 Persistent Reservation - Obsługa MPIO&MC/s, migawka/kopia zapasowm iSCI LUN

Zarządzanie prawami dostępu	- Ograniczenie dostępnej pojemności dysku dla użytkownika - Inportowanie listy użytkowników - Zarządzanie kontami użytkowników - Zarządzanie grupą użytkowników - Zarządzanie współdzieleniem w sieci - Tworzenie użytkowników za pomocą makr - Obsługa zaawansowanych ustawień dla podfolderów Windows ACL
Obsługa Windows Ad	Logowanie użytkowników do domeny poprzez CIFS, SMB, AFP, FTP oraz menedżera plików sieci WEB, Funkcja serwera LDAP
Funkcje backupu	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski ACL
Współpraca z zewnętrznymi dostawcami usług	Przynajmniej: Amazon S3, Amazon Glacier, Microsoft, Azure, Google Cloud Storage, Dropbox
Darmowe aplikacje na urządzenia mobilne	Monitoring/Zarządzanie/ Współdzielenie plików/ Obsługa kamer/ Odtwarzacz muzyki. Dostępne na systemy iOS, Android
Minimum obsługiwane serwery	- Serwer plików - Serwer FTP - Serwer WEB - Serwer baz danych MySQL - Serwer kopii zapasowych - Serwer iTunes - Serwer multimediów UPNP - Serwer wydruku - Serwer pobierania - Serwer monitoringu
VPN	VPN client / VPN Server, Obsługa PPTP, OpenVPN, L2TP
Konteneryzacja	Możliwość uruchomienia wirtualnych konteneró1.8. dla LXC i Docker
Administracja systemu	- Połączenia http / https - powiadamianie przez e-mail (uwierzytelnianie przez SMTP) - Powiadamianie przez SMS - DDNS oraz zdalny dostęp w chmurze, - SNMP (v2 i 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 - Możliwość ręcznej aktualizacji oprogramowania - Ustawienie Backup, przywracanie, resetowanie systemu
Zabezpieczenia	- Filtracja IP - Ochrona dostępu do sieci z automatycznym blokowaniem - Połączenie HTTPS - FTP z SSL/TSL (Explicit) - Obsługa SFTP (tylko admin) - Szyfrowanie AES 256-bit - Szyfrowana zdalna replikacja (Rsync poprzez SSH) - Import certyfikatu SSL - Powiadomienia o zdarzeniach za pośrednictwem e-mail i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami.
Gwarancja	Minimum 3 lata

1.7. Dysk twardy do dysku sieciowego

Nazwa komponentu	Wymagane minimalne parametry techniczne
Ilość	4 sztuki
Typ dysku twardego	HDD przystosowany do ciągłej pracy w urządzeniach typu NAS, kompatybilny z oferowanym serwerem NAS
Format	3,5” (LFF)
Typ napędu	Wewnętrzny
Pojemność dysku twardego	4 TB
Interfejs dysku twardego	SATA
Prędkość obrotowa	5400 obr./min.
Bufor	256 MB

1.8. Skaner dokumentów – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ skanera	Skaner będzie przeznaczony do codziennego skanowania dokumentów. Musi być wyposażony w automatyczny podajnik dokumentów ADF
Tryby skanowania	Skanowanie jednostronne lub dwustronne: w kolorze, w skali szarości, skan czarno-biały
Rodzaj czujnika skanowania obrazu	1-liniowy CMOS-CIS x2 (1 z przodu i 1 z tyłu)
Źródło światła	LED RGB x 2 (1 z przodu, 1 z tyłu)
Wykrywanie podwójnych pobrań	Ultradźwiękowy czujnik wykrywania podwójnych pobrań
Format dokumentów	Maksymalnie A4 pionowo (210 x 297 mm) lub Legal (8,5 x 14 cali) lub 215,9 x 863,6 mm (skanowanie długiego papieru: 3048 mm) Minimalne A8 w pionie/poziomie (52 x 74 mm)
Obsługiwana gramatura papieru	Papier o gramaturze od 50 do 209 g/m^2

Szybkość skanowania przy rozdzielczości 200, 300 dpi	W kolorze: - min. 20 stron jednostronnie - min. 40 stron dwustronnie W skali szarości: - min. 25 stron jednostronnie - min. 50 stron dwustronnie W czarno-białym: - min. 30 stron jednostronnie - min. 60 stron dwustronnie
Pojemność podajnika	Min. 50 arkuszy A4 (80 g/m2)
Interfejsy	USB, RJ-45
Funkcje przetwarzania obrazu	Automatyczne wykrywanie koloru, automatyczne wykrywanie rozmiaru strony, eliminacja przekosu, wiele obrazów, pomijanie pustych stron, rozpraszanie błędów, wygładzanie, podzielony obraz, redukcja pionowych smug, cyfrowe podpisywanie, wypełnienie krawędzi, korekcja krawędzi
Zużycie energii	W czasie użytkowania nie więcej niż 18 W lub mniej W trybie uśpienia nie więcej niż 1,6 W lub mniej W trybie Auto Standby (OFF) 0,4 W lub mniej
Kompatybilne systemy operacyjne	Windows® 10 (32-bit/64-bit), Windows® 8.1 (32-bit/64-bit), Windows® 7 (32-bit/64-bit), Windows Server® 2019 (64-bit), Windows Server® 2016 (64-bit), Windows Server® 2012 R2 (64-bit), Windows Server® 2008 R2 (64-bit), Windows Server® 2008 (32bit/64bit), Linux (Ubuntu)
Zgodność ze standardami środowiskowymi	ENERGY STAR®, RoHS
Elementy dołączone do zestawu	Podajnik ADF, kabel zasilający, zasilacz, kabel USB, płyta instalacyjna lub nośnik ze sterownikami

1.9. Zestaw konferencyjny – 10 szt.

Biurkowe rozwiązanie do obsługi wideokonferencji do niewielkich pokojów biurowych i biur. Konstrukcja typu wszystko w jednym, który obejmuje kamerę internetową typu „plug and play" o wysokiej rozdzielczości oraz zestaw głośnomówiący.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Kamera	Umożliwiająca połączenia wideo w rozdzielczości Full HD 1080p (do 1920 × 1080 pikseli); połączenia wideo w rozdzielczości HD 720p (do 1280 × 720 pikseli) Wysięgnik umożliwiający uniesienie kamery / umieszczenie kamery na poziomie oczu Technologia zapewniająca wyraźny obraz w różnych warunkach oświetleniowych, nawet przy słabym oświetleniu Dioda LED kamery wskazująca aktywne przesyłanie strumieniowe
Zestaw głośnomówiący	Zintegrowany dwukierunkowy zestaw głośnomówiący z usuwaniem echa i niwelacją szumów Przyciski sterowania odbieraniem/kończeniem połączeń, regulacji głośności, wyciszania i sterowania ruchem kamery Wbudowany mikrofon i głośniki
Kable	- Zasilacz - Kabel zasilania - Kabel USB
Uchwyt	Zaprojektowano do użycia na biurku
Zgodność	Zgodność z większością programów do wideokonferencji
Gwarancja	2 lata gwarancji na sprzęt

1.10 Tablet – 18 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Tablet	Urządzenie będzie wykorzystywane na potrzeby aplikacji biurowych, przeglądania Internetu i odbieraniu poczty elektronicznej. W ofercie należy podać nazwę producenta, typ, model oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację.
Ekran	Przekątna ekranu min. **10”** Dotykowy, minimum 10 punktowy o jasności min. 400 nitów, kąt widzenia minimum 160 stopni,
Rozdzielczość	Nie mniejsza niż FHD (1920x1200 px)
Procesor	Wielordzeniowy min. 8 rdzeni o częstotliwości min. 2,3 GHz

Kamera	Przednia kamera min. 5 MP Tylna kamera min. 8 MP
Pamięć operacyjna	Min 4 GB
Pamięć masowa	Min. 64 GB + slot MicroSD na dodatkową pamięć
Porty/złącza	Minimalna ilość dostępnych złącz: 1 x USB-C 1 x audio combo jack (3,5 mm)
WLAN + Bluetooth	Min AC + BT 5.0
WWAN	4G LTE
Czujniki	Akcelerometr, czujnik zbliżenia, czujnik Halla, czujnik światła, żyroskop
Bateria	Min. 7500 mAh, czas pracy min. 12 godzin
Waga	Max. 460 g
Certyfikaty i standardy	Energy Star 8.0 Rohs TÜV Rheinland Low Blue Light
Gwarancja	Min. 12 miesięcy
Dodatkowe wyposażenie	Zamykane Etui

1.11 Oprogramowanie do tworzenia kopii zapasowych – 1 szt.
Wymagania minimalne

a) Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
   - Microsoft Hyper-V min w wersjach 2019, 2016, 2012R2, 2012, 2008R2
   - VMware vSphere min w wersjach v4.1-7.0.2
   - Nutanix AHV 5.10, 5.15, 5.20 (LTS)
   - Maszyny fizyczne: Windows Serwer 2019, 2016, 2012R2, 2012, 2008R2
   - Microsoft 365 (Exchange online, One Drive for Business, Sharepoint)

b) Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vShpare, MS Hyper-V

c) Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:

- Na serwerze Windows lub Linux
- Jako maszyna wirtualna VMware
- Jako maszyna wirtualna Amazon
- Na serwerze NAS: Asustor, Netgear, Qnap, Synology, Western Digital

d) Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
e) Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
f) Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).

Licencjonowanie

a) Wszystkie funkcje i komponenty oprogramowania dla środowisk VMware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backapu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności.
b) Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwić rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska.
c) W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania.
d) W ramach dostawy wymagane jest dostarczenie licencji na ochronę **2** gniazd procesorów w hostach VMware lub Hyper-V.
e) Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dodatkowej licencji dla środowiska.
f) Wsparcie techniczne producenta i możliwość aktualizacji oprogramowania przez minimum 12 miesięcy.

Ochrona danych

a) Oprogramowanie musi posiadać funkcje backupu i replikacji:
    - Backup maszyn wirtualnych VMware
    - Replikacja maszyn wirtualnych VMware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu.
    - Backup maszyn wirtualnych Hyper-V
    - Replikacja maszyn wirtualnych Hyper-V (tworzenie /aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać tworzenia backupu.

- Możliwość określenia pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
- Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
- Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym.
  Kopia backupu(replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych.
- Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem.
- Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
- Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. Wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
- Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach.

Optymalizacja wykorzystania miejsca na dane

Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:

- Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
- Kompresja backupu, w tym konfigurowalny stopień kompresji
- Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne.

Spójność danych

a) Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
   - Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
   - Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
   - Automatyczne usuwanie (trunking) logów transakcyjnych z aplikacji: Microsoft exchange 2013, 2016, 2019, Microsoft SQL 2008, 2008R2, 2012, 2014, 2016, 2017, 2019
   - Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska VMware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki

- Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych VMware i Hyper-V
- Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
- Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji

Przywracanie danych

a) Oprogramowanie musi posiadać poniższe funkcje
- Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
- Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
- Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
- Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowania plików backupu): Microsoft Exchange, MS Active Directory, MS SQL,
- Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji VMware i Hyper-V i odwrotnie.

Wydajność

a) Oprogramowanie do backupu musi pozwalać na:
- Tworzenie backupu/replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
- Wykonywanie backupów przystosowanych bez wymogu okresowego tworzenia kopii pełnych
- Backup z pominięciem sieci LAN dzięki opcjom dostępu bezpośredniego w sieciach SAN
- Akceleracje sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
- Wsparcie dla urządzeń oferujących dodatkową deduplikację danych

Zarządzanie

a) Oprogramowanie musi pozwalać na następujące formy zarzadzania:
- Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
- Umożliwiać wysyłanie powiadomień w formie emaili dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej

- Zadanie backupu musi mieć możliwość uruchomienia zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
- Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzająw dysków do których będzie robiony eksport
- Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
- Oprogramowanie musi umożliwiać integrację z Active Directory
- Oprogramowanie musi wspierać tzw. Tryb multi tenant, umożliwiający podzielenie oprogramowania do backapu na kilka podinstalacji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach.

1.12 Oprogramowanie do szyfrowania (na 55 stacji roboczych)

Oprogramowanie musi posiadać następującą funkcjonalność:

a) Konsola centralnego zarzadzania musi wspierać systemy operacyjne Microsoft Windows Server 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit oraz Microsoft Windows 7/8/10/11 32-bit i 64-bit.
b) Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2005, 2008, 2012
c) Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI.
d) Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443.
e) Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish.
f) Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisania im różnych ról.
g) Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania.
h) Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła
i) Musi mieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzani, w oparciu o przynajmniej:
   - Ilość znaków
   - Czy hasło ma zawierać wielkie litery,
   - Czy hasło ma zawierać małe litery,
   - Czy hasło ma zawierać cyfry,
   - Czy hasło ma zawierać znaki specjalne
   - Okres ważności,
   - Ilość nieudanych logowań.
j) Administrator musi mieć możliwość konfiguracji złożoności haseł użytkowników na stacjach roboczych

k) Musi mieć możliwość konfiguracji złożoności hasa dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
   - Ilość znaków,
   - Czy hasło ma zawierać wielkie litery,
   - Czy hasło ma zawierać małe litery,
   - Czy hasło ma zawierać cyfry,
   - Czy hasło ma zawierać znaki specjalne
   - Okres ważności
   - Ilość nieudanych logowań
   - Możliwość zmiany hasła.

l) Konsola centralnego zarzadzania musi gromadzić informacje o:
   - Nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych,
   - Dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych
   - Dacie aktywacji klienta systemu szyfrowania danych,
   - Statusu szyfrowania,
   - Typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych,
   - Stanie polityki,
   - Wersji klienta systemu szyfrowania danych,
   - Wersji systemu operacyjnego stacji roboczej,
   - Użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej.

m) Konsola musi być dostępna z poziomu interfejsu www

n) Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet,

o) Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych.

p) Administrator musi mieć możliwość:
   - Instalacji klienta na stacji,
   - Zaszyfrowania/odszyfrowania stacji,
   - Wygenerowania klucza aktywacyjnego dla użytkownika,
   - Administrowania kluczami szyfrującymi,
   - Administrowania użytkownikami, którzy maja dostęp do stacji,
   - Administrowania profilem ustawień dla użytkowników,
   - Administrowania profilem ustawień dla stacji roboczej,
   - Wymuszenia zmiany hasła,
   - Zarządzania wieloma organizacjami z poziomu jednej konsoli,

Wymagania systemowe aplikacji Klienckiej

System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows Vista/7/8/10/11 32-bit i 64-bit oraz w środowiskach Microsoft Windows Serwer 2008 32-bit i 64 bit, 2012 64-bit, 2016 64-bit

Wymagania dotyczące uwierzytelniania

a) Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file)
b) Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows.

Wymagania dotyczące ustawień aplikacji klienckiej:

a) Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim,
b) Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób:
   a) Sektor po sektorze,
   b) Kontener
c) Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany ma dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła.
d) Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami,
e) Aplikacja musi umożliwiać automatyczna deszyfryzację otrzymanych wiadomości e-mail.
f) Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
g) Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczonego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania
h) Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.
i) Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania.
j) Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego.
k) Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego dokumentu, jego części, a także zawartości schowka systemowego.
l) Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła.
m) Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.
n) Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła.
o) Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów:
   a) Guttman.
   b) US Department of Defence 5220.22-M (8-306. /E).
   c) US Department of Defence 5220.22-M (8-306. /E, CiE).
   d) Kryptograficzne losowe dane liczbowe.
p) Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.
q) Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego.

r) Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie.
s) Aplikacja musi posiadać opcję automatycznego odpytania serwerów producenta o dostępność nowych wersji.
t) Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI.

Wymagania dotyczące szyfrowania

Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania:

a) AES (Rijndael)
b) Blowfish.
c) Triple DES (3Des)

Wymagania dotyczące licencji

Wymagane jest dostarczenie licencji na zaoferowane oprogramowanie na minimum 3 lata.

1.13 System logowania

Dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 6.5, 6.7, 7.0; Microsoft Hyper-V wersje: 2016, 2019, 2022; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

1. **Interfejsy, Dysk:**

    1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB.

2. **Parametry wydajnościowe:**

    1. System musi być w stanie przyjmować minimum 1 GB logów na dzień.
    2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

3. **Logowanie**

    1. Podgląd logowanych zdarzeń w czasie rzeczywistym.

2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

4. **Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

5. **Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.
   - Email.
   - IPS.
   - Traffic.
   - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

6. **Zarządzanie**

   a) System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
   Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
   b) System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

7. **Serwisy i licencje**

   a) System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
   b) Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

1.14 System do monitorowania 55 stacji roboczych

System do monitorowania 55 stacji roboczych (w tym urządzeń przenośnych), audytowania licencji, audytowania nieautoryzowanej instalacji nowego oprogramowania lub zmianie pierwotnej konfiguracji sprzętu czy problemach z jego funkcjonowaniem

Oprogramowanie musi posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli, agentów. Komunikacja pomiędzy wszystkimi modułami systemu musi być nawiązywana przy użyciu szyfrowanego protokołu TLS w wersji nie niższej niż 1.2. Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Oprogramowanie musi składować dane przy wykorzystaniu darmowego silnika bazy danych z kodem źródłowym dostępnym na licencji open-source, bez limitu ilości danych i bez konieczności nabycia dodatkowych licencji dla silnika bazy danych. Instalacja modułu Serwera oraz

Konsol zarządzających musi być możliwa na 64-bitowych systemach operacyjnych z rodziny MS Windows. Program Agenta musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbę usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje. Agent musi umożliwiać automatyczne wyszukanie serwera monitorującego stacje robocze.

Dane, które dotyczą działań użytkownika na komputerze, a więc: historia aktywności, polityka korzystania z zasobów Internetu, aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych technicznych tj. informacji o stacji roboczej. Dane te muszą być grupowane w osobnym, dedykowanym oknie i zgodne z RODO, musi istnieć możliwość usunięcia danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, musi być zgodny z RODO, czyli objęty kontrolą na poziomie wybranych konto administracyjnych poprzez nadawanie tym kontom różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników.

Główne konto administracyjne systemu musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną poprzez wyłączenie możliwość zdalnej deinstalacji Agenta, ograniczenie dostępu do Opcji programu oraz logów działań innych kont administracyjnych. Działania na kontach administracyjnych muszą być logowane do dzienników zawierających listę czynności wykonanych przez administratorów, w szczególności logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania kont administracyjnych muszą mieć możliwość automatycznie eksportowania do zewnętrznego kolektora Syslog.

Wymagane minimalne funkcjonalności (moduły) systemu:

Funkcjonalność (moduł) 1:

Bezagentowe monitorowanie infrastruktury obejmujące systemy Windows, Linux, Unix, Mac, ponadto urządzenia typu routery, przełączniki, urządzenia VoIP, drukarki sieciowe, UTM-y w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie PING oraz ARP-Ping,
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU),
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci,
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła w tym z wykorzystaniem jako tła zaimportowanych plików graficznych reprezentujących np. schemat rozmieszczenia pomieszczeń w budynku Urzędu,
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie,

- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny,
- zablokowania mapy urządzeń przed przypadkową edycją,
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów, z uwzględnieniem czas ich odpowiedzi i procentu utraconych pakietów,
- serwerów pocztowych: (czas logowania do serwisu odbierającego oraz czas wysyłania poczty)
- program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e--mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
- program ma możliwość wykonywania operacji testowych,
- program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa,
- monitorowania serwerów WWW i adresów URL,
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS,
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail,
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) - monitorowanie wartości za pomocą nazw zmiennych oraz OID,
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych,
- monitoringu routerów i przełączników wg: zmian stanu interfejsów sieciowych, ruchu sieciowego, podłączonych stacji roboczych z graficzną prezentacją panelu switcha, ruchu generowanego przez podłączone do portów stacje robocze,
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie / zatrzymanie / zrestartowanie,
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu,
- monitorowanie wydajności systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Program musi posiadać funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP. Program musi umożliwiać definiowanie alarmów z wykorzystaniem akcji związanych

ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie / restart usługi Windows, wyłączenie / restart komputera. Administrator musi mieć możliwość samodzielnego budowania alarmu poprzez wskazanie zdarzenia, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji które zostaną wykonane jako reakcja na wykryte zdarzenie. Program musi mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

Funkcjonalność (moduł) 2:

Inwentaryzacja, poprzez automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych, w tym:

1. Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart rozszerzeń.
2. Przygotowanie zestawienia posiadanych konfiguracji sprzętowych, wolnego miejsce na dyskach, średniego wykorzystania pamięci, informacji pozwalające na wytypowanie systemów, dla których konieczny jest wykonanie aktualizacji.
3. Informowanie o zainstalowanych aplikacjach oraz aktualizacjach systemów MS Windows.
4. Zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji / deinstalacji aplikacji, zmian adresu IP.
5. Wysyłanie powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
6. Odczytanie numeru seryjnego (klucza licencyjnego).
7. Automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
8. Przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
9. Utworzenie listy plików użytkowników z określonym rozszerzeniem, ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (np. wymiary obrazka), video (np. długość filmu), audio (np. długość nagrania), archiwów (np. liczba plików w archiwum, rozmiar po wypakowaniu).
10. Wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania tej funkcji muszą być logowane.
11. Prowadzenie bazy ewidencji zasobów IT w zakresie sprzętu i oprogramowania:

- przechowywania wszystkich informacji dotyczących infrastruktury IT oraz automatycznego aktualizowania zgromadzonych informacji,
- tworzenia powiązań między zasobami a urządzeniami,
- tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- wskazania osób uprawnionych do użycia zasobów,
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości poprzez możliwość dodawania dodatkowych informacji takich jak: numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (z możliwością zdefiniowania daty, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, własny komentarz,
- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),
- przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu,
- tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczania statusów zasobów (minimum): w użyciu, w naprawie, zutylizowany,
- ewidencji czynności wykonywanych na zasobach: aktualizacja, naprawa w serwisie, konserwacja wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- generowania protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i herb Gminy,
- archiwizacji i porównywania audytów zasobów,
- tworzenia kodów kreskowych dla zasobów,
- drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,

- inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej na system Android,
- inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu "data" z atrybutów zasobów lub licencji.

Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji
o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów.
2. Informacje o aplikacjach używanych w Urzędzie.
3. Tworzenie własnych wzorców aplikacji.
4. Tworzenie dowolnie nazwanych kategorii aplikacji.
5. Informacje o komputerach, na których aplikacja została wykryta.
6. Zarządzanie posiadanymi licencjami.
7. Wskazywanie osób odpowiedzialnych za licencję.
8. Wskazanie użytkowników licencji.
9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
10. Zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie według różnych wersji aplikacji na jednym urządzeniu.
11. Łatwy audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji.
12. Zarządzanie posiadanymi licencjami - generowanie raport zgodności licencji.
13. Możliwość przypisania do programów numerów seryjnych, wartości.

Program musi posiadać Agenta inwentaryzacji wspierającego proces inwentaryzacji instalowanego na systemie Android.

Funkcjonalność (moduł) 3:

Monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

1. Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy).
2. Procesów wraz informacją o ich uruchomieniu na podwyższonych uprawnieniach.
3. Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność.
4. Informacji o edytowanych przez użytkownika dokumentach.
5. Historii pracy w tym poprzez cykliczne zrzuty ekranowe.
6. Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczba i czas odwiedzin).
7. Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika).
8. Wydruków (minimum): informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Monitorowanie kosztów wydruków.
9. Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program musi posiadać możliwość wprowadzenia restrykcji takich jak:

1. Blokowanie stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków - zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen muszą mieć możliwość tworzenia dla użytkownika lub grupy użytkowników i być kopiowane pomiędzy grupami lub kontami.
2. Blokowanie ruchu na wskazanych portach TCP/IP.
3. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,

Program musi posiadać możliwość informowania poprzez:

1. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy (domeny), pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet, wydrukuje określoną ilość stron w ciągu dnia.
2. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu.
3. Generowanie raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

4. Program musi mieć możliwość definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Funkcjonalność (moduł) 4:

Realizacja pomocy zdalnej użytkownikom stacji roboczych w ramach którego:

1. Dostępny musi być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie z opcją odrzucenia takiego połączenia przez użytkownika.
2. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran.
3. Administrator w trakcie zdalnego dostępu musi mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika.
4. Moduł musi dawać możliwość prowadzenia bazy zgłoszeń umożliwiającej użytkownikom zgłaszanie problemów technicznych, przetwarzana i przyporządkowywana zgłoszeń odpowiednim administratorom, z mechanizmem automatycznego powiadomienia.
5. Moduł musi umożliwiać również przetwarzanie zgłoszeń w trybie anonimowym według wymogów "Dyrektywy o sygnalistach".
6. Moduł musi umożliwiać użytkownikom monitorowanie procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron.
7. Moduł musi zawierać wbudowany komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów).
8. Moduł musi umożliwiać użytkownikom uzyskanie dostępu z prywatnego komputera do wcześniej zdefiniowanego komputera Urzędu który zlokalizowany jest w sieci Urzędu, za pomocą funkcji zdalnego dostępu.
9. Moduł musi umożliwiać zbudowanie i prowadzenie bazy wiedzy.
10. Moduł pomocy zdalnej musi dawać możliwość:
    - pobierania listy użytkowników z Active Directory,
    - zarządzania lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
    - zarządzanie dostępem pracowników do zgłoszeń pomocy technicznej,
    - zarządzanie dostępem do czatu w na minimum 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,

- tworzenia własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii, opisami kategorii oraz klauzulą RODO,
- automatycznego przypisywania konkretnych pracowników pomocy technicznej do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
- procesowania zgłoszeń użytkowników z wiadomości e-mail,
- tworzenia formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
- wykonywania operacji na wielu zgłoszeniach równocześnie,
- dołączania załączników do zgłoszeń,
- wyszukiwania zgłoszeń i artykułów w bazie wiedzy,
- szybkiego dostępu do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
- wprowadzenia komentarzy oraz informacji przy zamykaniu zgłoszenia,
- wykonywania zrzutów ekranowych (podgląd pulpitu),
- dystrybucji oprogramowania przez Agenta (Agentów),
- dystrybucji oraz uruchamiania plików za pomocą Agentów (w tym plików MSI) - (jeśli komputer jest wyłączony w trakcie zlecania operacji musi nastąpić jego kolejkowanie)
- planowania nieobecności pracowników pomocy technicznej,
- obsługi umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami o przekroczeniach SLA,
- generowania raportów obsługi pomocy technicznej,
- zdalne wykonywanie poleceń poprzez Agentów (utworzenie / edycja konta lokalnego użytkownika systemu),
- zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
- wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

Funkcjonalność (moduł) 5:

Ochrony danych przed wyciekiem poprzez:

1. Blokowanie urządzeń i nośników danych.

2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazd kart pamięci, SATA, dysków przenośnych, napędów CD/DVD, stacji dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokowanie tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) nie mogą być blokowane.
5. Alarmowanie o zdarzeniach podłączenia / odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Integracja i zarządzanie ustawieniami Windows Defender.
7. Monitorowanie stanu szyfrowania dysków funkcją BitLocker.
8. Monitorowanie stanu modułu TPM.
9. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.
10. Integracje z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień do kont użytkowników lokalnych.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników / grup do odczytu, zapisu, wykonania plików.
2. Autoryzowanie urządzeń zdefiniowanych, będących własnością Urzędu: pamięci USB, dysków - blokowanie urządzeń prywatnych.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy zaufanych urządzeń nośników wycofanych z eksploatacji.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie / odłączenie urządzenia przenośnego.

Oprogramowanie musi posiadać możliwość utworzenia platformy informacyjnej (na potrzeby Security Operation Center) która w oparciu o witrynę WWW, pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety muszą być rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych musi być automatycznie odświeżana oraz mieć możliwość udostępniana w trybie "tylko do odczytu" z zabezpieczeniem tokenem, platforma musi mieć możliwość wyświetlana w trybie jasnym

lub ciemnym. Widgety muszą prezentować dane ze modułów funkcjonalnych oprogramowania w zakresie nie mniejszym niż: liczniki wydajności, alarmy oraz odpowiedzi serwisów TCP/IP, zmiany w konfiguracji sprzętowej urządzeń z Agentami, zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, alarmy dla zasobów, statystyki wydruków, statystki użycia aplikacji, statystki użycie łącza, aktywność na stronach WWW, statystyki z obsługi zgłoszeń, lista najnowszych nierozwiązanych zgłoszeń, lista najstarszych nierozwiązanych zgłoszeń, ostatnio podłączone nośniki zewnętrzne, ostatnie operacje na plikach (wraz z filtrowaniem), produktywność dla grupy, Statystyki czasu nieproduktywnego.

2 Konfiguracja i uruchomienie sprzętu

2.1. Wymagania ogólne

Wszystkie dostarczane urządzenia muszą zostać zainstalowane (tj. wypakowane, zmontowane, zamontowane w szafach RACK, uruchomione i skonfigurowane]) w docelowym miejscu pracy (wskazanym przez Zamawiającego) w terminie uzgodnionym z Zamawiającym (miejsce i termin instalacji należy uzgodnić na min. 5 dni roboczych przed planowaną dostawą urządzeń). Wszystkie opakowania zostaną zutylizowane przez i na koszt Wykonawcy.

Serwery oraz dysk sieciowy dostarczone w ramach tego postępowania przeznaczone do instalacji w szafie RACK, muszą być zainstalowane w szafie RACK.

Zamawiający wydzieli pomieszczenie pod instalację infrastruktury, Wykonawca zainstaluje sprzęt w pomieszczeniu zgodnie z zaleceniami producenta dot. warunków pracy dla dochowania warunków gwarancji pod względem parametrów fizycznych otoczenia i zadba o spełnienie warunków fizycznych dla bezpieczeństwa instalowanej infrastruktury min. w okresie udzielonej gwarancji. Pomieszczenie jest klimatyzowane. W celu prawidłowego oszacowania warunków i zakresu prac instalacyjnych w pomieszczeniu Zamawiający zaleca wykonanie wizji lokalnej.

2.2. Serwery

Na serwerach należy zainstalować system wirtualizacji i skonfigurować go do korzystania z zasobów dyskowych dysku sieciowego. Wykonawca zaprojektuje schemat rozmieszczeń, ilości i przydział zasobów dla wszystkich serwerów wirtualnych wymaganych do realizacji Przedmiotu Zamówienia. Wykonawca zaprojektuje i wdroży system backupu min. maszyn wirtualnych. Wykonawca wdroży (tj. zainstaluje, uruchomi, skonfiguruje i przetestuje) infrastrukturę zapasową serwerów wirtualnych oraz procedurę przełączania usług. Na serwerze fizycznym Wykonawca utworzy infrastrukturę serwerów wirtualnych. Serwery wirtualne należy skonfigurować do korzystania z zasobów sieciowych i dyskowych. Wszystkie maszyny wirtualne muszą zostać skonfigurowane zgodnie z ich przeznaczeniem (np. DHCP, DNS, SQL, IIS, SMB, etc.). Wszystkie możliwe protokoły sieciowe [ssh, http, https, telnet, itp.] muszą zostać zabezpieczone przed niepowołanym dostępem.

2.3. System zarządzana uprawnieniami użytkowników – Domena

Wykonawca zainstaluje i skonfiguruje system domeny na instalowanej infrastrukturze sprzętowej zgodnie z zaleceniami producenta systemu domeny oraz zgodnie ze strukturą organizacyjną Urzędu i utworzy

konta użytkowników Urzędu. Wykonawca w uzgodnieniu z Zamawiającym ustali zasady grup jakie należy zaimplementować i wdroży je.

Podpięcie komputerów będzie obowiązkiem Zamawiającego ale Wykonawca musi świadczyć usługę asysty w przypadku problemów.

2.4. Kopie zapasowe

Wykonawca we współpracy z ASI opracuje politykę kopii bezpieczeństwa uwzględniającą możliwości techniczne po wdrożeniu Projektu. Na podstawie polityki Wykonawca skonfiguruje systemy i usługi do wykonywania kopii bezpieczeństwa zgodnie z harmonogramami. Przetestuje działanie mechanizmu automatycznego wykonywania kopii bezpieczeństwa. W ramach wdrożenia musi zostać dostarczona instrukcja odtwarzania danych w różnych zakresach (np.: pojedynczy plik, cały katalog, użytkownik wraz z plikami, maszyna, itp.). Wszystkie kopie muszą być zapisywane min. na serwerze kopii. Serwer kopii zapasowych musi zostać zainstalowany w serwerowni. Zasoby serwera kopii posłużyć mają do bezpiecznego przechowywania kopii bezpieczeństwa systemów zainstalowanych w serwerowni. Serwer musi zostać podłączony do sieci wewnątrz serwerowej.

3. Gwarancja i serwis

Zamawiający wymaga udzielenia gwarancji, terminów licencji i wsparcia technicznego, zgodnie ze złożoną ofertą oraz warunkami podanymi poniżej.

1. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów lub ich autoryzowanych partnerów.
2. Wykonawca dostarczy wraz z towarem dokument gwarancji, jakości sprzętu wystawiony przez siebie lub producenta urządzenia, zobowiązujący wystawcę dokumentu (gwaranta) do usunięcia wady fizycznej towaru lub do dostarczenia towaru wolnego od wad, jeżeli wady te ujawnią się w ciągu terminu obowiązywania gwarancji. Dokument wystawiony przez Wystawcę dokumentu (gwaranta) musi odzwierciedlać wykupione pakiety gwarancyjne i serwisowe u producenta lub jego autoryzowanych dystrybutorów o ile oferent nie posiada takiej autoryzacji
3. Okres gwarancji, który Wykonawca udzieli Zamawiającemu, będzie zgodny ze złożoną ofertą, lecz nie krótszy niż wyspecyfikowany dla poszczególnych urządzeń i oprogramowania.
4. Bieg okresów gwarancyjnych rozpoczyna się z dniem podpisania Protokołu Odbioru Końcowego bez uwag (zastrzeżeń).
5. Czas naprawy wyłączony będzie z okresu gwarancyjnego. Czas trwania gwarancji zostanie automatycznie wydłużony o czas trwania naprawy.
6. Wykonawca udziela Zamawiającemu (24 miesięcznej) gwarancji na bezawaryjne działanie wszelkich nośników instalacyjnych.
7. W okresie gwarancji, wszelkie koszty związane z usunięciem awarii, w tym dostarczenie uszkodzonego sprzętu do punktu serwisowego, obciążają gwaranta.

8. Gwarancja obejmie wszystkie wykryte podczas eksploatacji sprzętu usterki i wady oraz uszkodzenia powstałe w czasie poprawnego zgodnego z instrukcją użytkowania.
9. Zasady eksploatacji i konserwacji urządzeń zostaną określone w przekazanej przez wykonawcę „Instrukcji użytkowania i eksploatacji urządzeń" wraz z wykazem urządzeń, które wymagają przeglądów serwisowych.
10. W przypadku awarii sprzętu, która nie została usunięta w terminie 30 dni, Wykonawca zobowiązuje się do wymiany sprzętu na nowy o parametrach nie gorszych od sprzętu uszkodzonego. Wymiana sprzętu na nowy nastąpi najpóźniej w 35 dniu od zgłoszenia.
11. Wykonawca zapewni możliwość zgłaszania awarii sprzętu w okresie gwarancji telefonicznie, faksem oraz drogą mailową w godzinach od 08.00 do 16.00 od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy. Zgłoszenie awarii po godz. 16.00 będzie traktowane, jak zgłoszenie o godz.08.00 następnego dnia roboczego.
12. Wykonawca musi podjąć czynności serwisowych w czasie nieprzekraczającym jednego dnia roboczego od momentu zgłoszenia o ile nie wymaga szybszej reakcji minimalny czas opisany w przedmiocie zamówienia.
13. W przypadku stwierdzenia wady ukrytej sprzętu (towaru) wykonawca musi wymienić go na nowy, w ciągu 14 dni roboczych od daty zgłoszenia tej wady.
14. Serwis gwarancyjny świadczony będzie w miejscu użytkowania sprzętu.
15. W przypadku, kiedy Wykonawca uzna za konieczna naprawę sprzętu w serwisie, gwarant zapewni:
    a) Odbiór na własny koszt wadliwego sprzętu (towaru) w terminie nieprzekraczającym 2 dni roboczych;
    b) Dostawę naprawionego sprzętu na własny koszt w terminie nie przekraczającym 2 dni roboczych od dnia usunięcia awarii przez serwis, a w uzasadnionych przypadkach w terminie nie dłuższym niż 14 dni roboczych od odebrania sprzętu z siedziby zamawiającego.
    c) W przypadku braku możliwości usunięcia awarii w terminie 14 dni roboczych od dnia odebrania wadliwego sprzętu (towaru) z siedziby zamawiającego, wykonawca zobowiąże się do bezpłatnego dostarczenia i uruchomienia nowego sprzętu zastępczego o parametrach równoważnych z oferowanymi. Podstawiony sprzęt będzie miał zainstalowany uzgodniony z Zamawiającym system operacyjny i wszystkie dodatkowe, standardowe poprawki niezbędne do jego poprawnej pracy.
16. Koszt dojazdu ekipy serwisowej w ramach napraw gwarancyjnych i koszty transportu sprzętu naprawianego w ramach gwarancji pokryje wykonawca.

Oferowane przez Wykonawcę w dniu składania ofert rozwiązania, nie mogą być przeznaczone przez ich producenta do wycofania z produkcji, sprzedaży lub z wsparcia technicznego. Oferowane urządzenia

muszą być przypisane w serwisie producenta do Zamawiającego.

Zamawiający wymaga, aby dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień składania ofert.

W celu potwierdzenie spełnienia przez oferowany sprzęt wskazanych w niniejszym dokumencie wymagań, Wykonawca na wezwanie Zamawiającego przedłoży szczegółowy wykaz oferowanego sprzętu, użyte do realizacji zamówienia komponenty, karty katalogowe lub inną dokumentację techniczną z zaznaczeniem na nich wyspecyfikowanych parametrów. Dodatkowo w przypadku dedykowanego montażu własnego Wykonawca przedstawi oświadczenie producenta sprzętu lub inny dokument poświadczający, że Wykonawca posiada autoryzacje producenta na dokonywanie modyfikacji konfiguracyjnych sprzętu i że taka modyfikacja nie ma wpływu na ewentualne świadczenia gwarancyjne.

4. Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji projektowej realizacji każdego zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji umowy.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierająca opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego (platformy sprzętowej, systemowej, bazodanowej i aplikacyjnej). Dokumentacja musi zawierać wszystkie dane pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresem dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania danego elementu Systemu w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył Politykę backupu i archiwizacji zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów.

Dokumentacja musi być sporządzona w języku polskim i dostarczona w wersji elektronicznej z możliwością przeszukiwania treści.

Zawartość Dokumentacji musi być zgodna z wytworzonym Rozwiązaniem.

Zamawiający zezwala na dostarczenie dokumentacji w formie pomocy kontekstowej wbudowanej w GUI.

Dokumentacja administratora

1. Dokumentacja Administratora Rozwiązania musi opisywać kolejność czynności i zakres możliwych danych do wprowadzenia oraz sposób postępowania w sytuacjach szczególnych i awaryjnych.

2. Dokumentacja Administratora Rozwiązania powinna być dostępna w postaci elektronicznej umożliwiającej przeszukiwanie oraz odnajdywanie konkretnych tematów.

3. Dokumentacja Administratora Rozwiązania obejmować będzie, co najmniej:

a. szczegółową (krok po kroku) instrukcję instalacji i konfiguracji Rozwiązania

b. opis parametrów instalacyjnych i konfiguracyjnych Rozwiązania wraz z opisem dopuszczalnych wartości i ich wpływem na działanie rozwiązania,

c. szczegółową (krok po kroku) instrukcję wgrywania nowych wersji Rozwiązania,

d. szczegółowy opis możliwych do zastosowania ról i uprawnień wraz z ich wpływem na działania rozwiązania.

4. Zamawiający wymaga przekazania w bezpiecznej formie wszystkich loginów i haseł umożliwiających samodzielne zarządzanie wszystkimi usługami (również zadań serwisowych).

Dokumentacja powykonawcza

Wykonawca jest zobowiązany dostarczyć Dokumentację powykonawczą, która musi być sporządzona zgodnie z poniższym szablonem, przy czym szablon może zostać uzupełniony o dodatkowe elementy przez Wykonawcę:

1. Opis wdrożonych systemów i aplikacji.

1.1. Opis systemu.

1.2. Funkcjonalności

1.3. Zależność pomiędzy wszystkimi elementami Rozwiązania.

2. Opis przepływu danych pomiędzy poszczególnymi Modułami wraz ze schematami graficznymi.

3. Sposób instalacji i konfiguracji Rozwiązania:

4. Wymagane licencje - wykaz niezbędnych licencji.

5. Karty gwarancyjne.

Część II: Zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem w ramach projektu „Wsparcie dzieci i rodzin pegeerowskich w rozwoju cyfrowym - Granty PPGR”

Laptop – 26 szt.

Komputer przenośny (laptop).

W ofercie należy podać nazwę producenta, typ, model oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.

Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego.

Nie dopuszcza się zaoferowania komputera refurbished.

Nie dopuszcza się modyfikacji na linii producent-Zamawiający.

Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej specyfikacji. W tym celu wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez komisję przetargową na zasadzie spełnia/nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki z treścią specyfikacji. Niezgodność próbki ze specyfikacją chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek.

Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.

Nazwa komponentu	**Wymagane minimalne parametry techniczne komputerów**
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej 6200 punktów na podstawie PassMark PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie powinien podać dokładny model oferowanego podzespołu. Procesor wykonany w litografii nie większej niż 10nm. (Do oferty należy załączyć wydruk z przeprowadzonych testów na konfiguracji identycznej z zaoferowaną lub link do strony producenta testu z opublikowanym wynikiem).
Pamięć operacyjna RAM	Min. 8 GB, rodzaj pamięci DDR4 min. 3200MHz
Parametry pamięci masowej	Min. 256 GB SSD NVMe, zawierający partycję Recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość rozbudowy do konfiguracji dwudyskowej w oparciu o dysk M.2 SSD oraz 2,5”. Dopuszcza się również rozwiązania posiadające 2

	złącza M.2 dla dysków SSD. W Przypadku dysku 2,5” gotowa do rozbudowy zatoka umożliwiająca podłączenie dysku.
Karta graficzna	Zintegrowana
Wyposażenie multimedialne	Wbudowana karta dźwiękowa zgodna z HD Audio, wbudowane głośniki stereo Dolby Audio min 2x1,5W, wbudowany mikrofon, sterowanie głośnością za pośrednictwem wydzielonych klawiszy funkcyjnych na komputerze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), wbudowana kamera internetowa z wbudowaną przesłoną.
Obudowa	Obudowa wyposażona w zawiasy metalowe. Nie dopuszcza się demontowanych zasłon kamery. Kąt otwarcia matrycy min 176 stopni. W obudowę wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego lub stan pracy komputera.
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. Płyta główna i konstrukcja laptopa wspierająca konfigurację dwu dyskową SSD M.2 + (HDD 2,5” lub SSD 2,5”)
Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
Bezpieczeństwo	Zintegrowany układ TMP 2.0
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w PIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość odczytywania z BIOS bez utraty systemu operacyjnego z dysku twardego lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS - numer seryjny komputera - ilość pamięci RAM - typie procesora - zainstalowanym dysku - o zintegrowanej w BIOS nazwy producenta komputera oraz modelu lub

	konfiguracji zaoferowanej jednostki. Nie dopuszcza się wykonania pól Asset TAG w BIOS do propagacji w/w informacji. Administrator z poziomu BIOS musi mieć możliwość wykonywania poniższych czynności: Możliwość ustawienia: - hasła dla dysku twardego - hasła Administratora oraz Użytkownika - kolejności bootowania - włączania/wyłączania WiFi - włączania/wyłączania wirtualizacji - włączania/wyłączania wgrywania starszej wersji BIOS - sposobu działania klawiszy F1-F12 (normalna praca/skróty) - trybu wydajności lub chłodzenia W przypadku występowania na klawiaturze przycisku Fn wymaga się funkcjonalności w BIOS umożliwiającej zamianę funkcji pomiędzy klawiszami Ctrl i Fn, tak aby użytkownik nie musiał zmieniać swoich przyzwyczajeń umiejscowienia przycisków Ctrl i Fn, co wpływa na komfort obsługi. Przy ustawionym haśle Administratora, zalogowany Użytkownik do BIOS musi mieć możliwość zmiany własnego hasła. Nie dopuszcza się możliwości edycji ustawień wpływających na bezpieczeństwo urządzenia. Możliwość ustawienia portów USB w trybie „no Boot", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.
Ekran	Matryca min 15,6" z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare, rozdzielczość: FHD 1920x1080, jasność min. 250 nitów.
Interfejsy/ komunikacja	Min. 3 porty USB z czego min 2xUSB 3.2 min. 1 złącze typu C, złącze słuchawek i złącze mikrofonu typu Combo, RJ-45, HDMI. Złącze HDMI musi umożliwić podłączenie i obsługę zewnętrznego wyświetlacza w rozdzielczości min. 3840x2160 przy min. 30Hz
Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AC 1x1 Bluetooth 5.0

Klawiatura	Klawiatura w układzie US, odporna na zalanie z wydzielonym blokiem numerycznym. (Zamawiający wymaga dostarczenia karty katalogowej producenta potwierdzającej odporność klawiatury na zalanie cieczą)
Wbudowany akumulator	Pozwalający na nieprzerwalną pracę przez min. 5,5 godziny, MobileMark 2018
Zasilacz	Zasilacz zewnętrzny 65 W
Certyfikaty oświadczenia i standardy	- Certyfikat ISO9001 dla producenta sprzętu (należy dołączyć do oferty) - Deklaracja zgodności CE (załączyć do oferty) - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta odnoszący się do zaoferowanej jednostki.
Waga	Waga urządzenia z baterią podstawową poniżej 1,7 kg
System operacyjny	Microsoft Windows 11 Pro 64 bit lub inny system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: Poziom menu, poziom otwartego okna systemu operacyjnego, system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 9. Wbudowany system pomocy w języku polskim 10. Możliwość przystosowania środowiska dla osób niepełnosprawnych (np. słabo widzących)

	11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez Administratora systemu Zamawiającego 12. Możliwość dostarczania poprawek do systemu operacyjnego modelu peer-to-peer 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie, praca systemu w trybie ochrony kont użytkowników 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchomienia wybranej aplikacji – tryb „kiosk” 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. Quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie do tworzenia kopii zapasowych (Backup), automatyczne wykonywanie kopii plików z możliwością automatycznego przywracania wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 24. Wbudowany mechanizm wirtualizacji typu hypervisor 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.

	27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania uprawnieniami zapory i regułami IPv4 i IPv6 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa(z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści pomiędzy aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelniania dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnianie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TMP 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrożenie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a) Login i hasło b) Karty inteligentne i certyfikaty (smartcard) c) Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chronione poprzez moduł TMP) d) Certyfikat/Klucz i PIN e) Certyfikat/Klucz i uwierzytelnianie biometryczne 39. Wsparcie dla uwierzytelnienia na bazie Kerberos v5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x, 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchomienia interpretera poleceń

	43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń Licencja systemu operacyjnego zaimplementowana w BIOS komputera, umożliwiająca instalację systemu bez podawania klucza aktywacji systemu za pośrednictwem Internetu. Nie dopuszcza się zaoferowania systemu operacyjnego typu refurbished.
Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania dołączonego przez producenta w tym również wgranie nowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizację i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
Oprogramowanie biurowe	Oprogramowanie biurowe MS Home & Business 2021 w wersji Polskiej z licencją wieczystą lub oprogramowanie równoważne zawierające minimum: •arkusz kalkulacyjny, •edytor tekstu, •program do tworzenia prezentacji, Programy wchodzące w skład pakietu muszą w 100% odwzorowywać treść i układ dokumentów doc, docx, rtf, xls, xlsx, ppt, pptx wytworzonych w posiadanych przez Zamawiającego pakietach Microsoft Office od wersji 2013 Edytor tekstu musi poprawnie odwzorowywać wszystkie elementy umieszczone w nagłówkach i stopkach dokumentów DOC oraz DOCX, obsługiwać osadzanie innych dokumentów tekstowych oraz arkuszy kalkulacyjnych. Dla wstawianych obiektów typu „wykres” musi istnieć możliwość osadzenia danych służących do utworzenia tego wykresu z możliwością ich edycji bezpośrednio z edytora tekstu lub poprzez otwarcie danych w dostarczanym arkuszu kalkulacyjnym. Edycja 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. Śledzenie zmian wprowadzonych przez użytkowników. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do

	zarządzania informacją prywatną. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Arkusz kalkulacyjny musi umożliwiać użycie wszystkich funkcji dostępnych w posiadanym przez Zamawiającego oprogramowaniu Microsoft Excel od wersji 2013. Arkusz kalkulacyjny musi zawierać (lub umożliwiać doinstalowanie bezpłatnego dodatku) oprogramowanie umożliwiające zoptymalizować wartość komórek zmienianych w celu uzyskania oczekiwanego rezultatu końcowego, przy jednoczesnym spełnieniu wszystkich zdefiniowanych parametrów oraz ograniczeń. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe ora formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową analizę wariantową i rozwiązywanie problemów optymalizacyjnych. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynność. Formatowanie czasu, daty i wartości finansowych z polskim formatem. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Program do prezentacji musi poprawnie obsługiwać wszystkie animacje i przejścia utworzone w posiadanym przez Zamawiającego programie Microsoft Power Point od wersji 2013. Program musi umożliwiać prezentowanie przy użyciu projektora multimedialnego. Drukowanie w formacie umożliwiającym robienie notatek. Zapisanie jako prezentacja tylko do odczytu, nagrywanie narracji i dołączanie jej do prezentacji, opatrywanie slajdów notatkami dla prezentera. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, tabel i wykresów pochodzących z arkusza kalkulacyjnego. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. Możliwość tworzenia animacji obiektów i całych slajdów. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym, monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
Antywirus	Oprogramowanie antywirusowe z licencją na 3 lata.

	Minimalne techniczne, funkcjonalne i użytkowe wymagania dotyczące oprogramowania antywirusowego: 1. Ochrona stacji roboczych - z zainstalowanym systemem operacyjnym Windows a) Pełne wsparcie dla systemu Windows 7/8/8.1/10/11 b) Wsparcie dla 32 i 64 bitowej wersji systemu Windows c) Wersja programu dostępna w języku polskim d) Pomoc w programie i dokumentacja dostępna w języku polskim 2. Ochrona antywirusowa i antyspyware • Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami • Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. • Wbudowana technologia do ochrony przed rootkitami. • Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. • Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. • Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu. • System musi posiadać możliwość definiowania zadań w harmonogramie • Skanowanie „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym systemu operacyjnego • Możliwość skanowania dysków sieciowych i dysków przenośnych. • Możliwość skanowania plików spakowanych i skompresowanych. • Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. • Użytkownik musi posiadać możliwość tymczasowego wyłączenia oprogramowania. • Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. • Skanowanie ruchu http na poziomie stacji roboczej. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlone jest stosowne powiadomienie. • Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń. • Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.

	• Możliwość podejrzenia informacji o licencji, która znajduje się w programie. • W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być zainstalowane.
Gwarancja	Minimalny czas trwania gwarancji producenta wynosi 3 lata, świadczona w miejscu użytkowania sprzętu (on-site). Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – Zamawiający zastrzega sobie prawo do możliwości weryfikacji powyższego wymogu. W przypadku weryfikacji przez Zamawiającego, Wykonawca dostarczy stosowne dokumenty pochodzące od producenta komputera. Wymagane oświadczenie producenta komputera, że w przypadku nie wywiązania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Wsparcie techniczne producenta	▪ Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera. ▪ Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00 do 18:00 ▪ Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. ▪ Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.

Część III: Przeprowadzenie szkoleń stacjonarnych z obsługi sprzętu komputerowego, cyberbezpieczeństwa, przeprowadzenie dwóch audytów zgodności z KRI i RODO i dwóch testów penetracyjnych systemów informatycznych w Urzędzie Miasta i Gminy w Chmielniku w ramach projektu „Cyfrowa Gmina"

Zadanie 1. Szkolenie stacjonarne dla pracowników Urzędu Miasta i Gminy w Chmielniku w zakresie obsługi zakupionego sprzętu i oprogramowania

1) Szkolenie zostanie przeprowadzone w formie stacjonarnej (w siedzibie Zamawiającego) prezentacji i wykładu dla dwóch osobnych grup maksymalnie do 30 osobowych;

2) Czas trwania szkolenia dla każdej z grup - do 1,5h + 30min (ewentualna dyskusja i zadawanie pytań);

3) Tematyka szkolenia będzie dotyczyła min. zagadnień z zakresu:
- obsługi pakietu biurowego: WORD, Excel,
- wysyłki poczty elektronicznej,
- szyfrowania dokumentów WORD, Excel, pdf, tworzenia dokumentu do pliku pdf,

Termin realizacji: listopad 2022 r.

Zadanie nr 2. Szkolenie dla pracowników Urzędu Miasta i Gminy w Chmielniku w zakresie cyberbezpieczeństwa

1) Szkolenie zostanie przeprowadzone w formie stacjonarnej (w siedzibie klienta) prezentacji i wykładu dla dwóch osobnych grup maksymalnie do 30 osobowych;

2) Czas trwania szkolenia dla każdej z grup - do 1,5h + 30min (ewentualna dyskusja i zadawanie pytań);

3) Tematyka szkolenia będzie dotyczyła min. zagadnień z zakresu cyberbezpieczeństwa tj. :

- ochrona danych osobowych,

- zagrożenia dla użytkownika i zasobów organizacji;

- socjotechniczne mechanizmy działania cyberprzestępców;

- rozpoznawanie zagrożeń oraz reagowanie na pojawiające się niebezpieczeństwa;

- dobre praktyki zabezpieczania się przed poszczególnymi zagrożeniami;

- utrzymanie bezpieczeństwa informacji w systemach informatycznych (zabezpieczanie środowiska pracy)

- podstawy bezpieczeństwa systemów informatycznych;

- przenoszenie się zagrożeń pomiędzy obszarem prywatnym a służbowym;

- profilaktyka bezpiecznego korzystania z Internetu oraz sieci LAN i Wi-Fi,

- konsekwencje lekceważenia zasad cybezpieczeństwa;

4) Do dyspozycji zamawiającego zostaną przekazane w formie elektronicznej materiały obejmujące tematykę szkolenia.

5) Wykonawca oświadcza, że posiada potencjał techniczny, osobowy, wiedzę oraz doświadczenie niezbędne do wykonania przedmiotu zamówienia – konieczne wykazanie przez wykonawcę, że w okresie ostatnich 3 lat wykonywane były przez niego szkolenia z zakresu cyberbezpieczeństwa lub

bezpieczeństwa pracy w systemach informatycznych, w co najmniej 6 jednostkach samorządu terytorialnego.

Termin realizacji:
1. Szkolenie nr 1 – październik 2022 r.
2. Szkolenie nr 2 – styczeń 2023 r.

Zadanie nr 3. Przeprowadzenie audytów w jednostce zgodności z KRI i RODO

Przeprowadzenie dwóch audytów - ocenę dostosowania systemu zarządzania bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Chmielniku do wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI) (t.j. Dz.U. z 2017 r., poz. 2247), Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.). w tym legalności oprogramowania, testy penetracyjne, audyt bezpieczeństwa informacji, ocenę dostosowania systemu zarządzania bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Chmielniku do wymagań RODO;

2/ W oparciu o raport z audytu przedstawienie rekomendacji dostosowującej stosowną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji do spełnienia wymogów KRI, RODO oraz PN-ISO/IEC 27001 lub późniejszej.

Audyt (przegląd i ocena)

Cel audytu

Audyt w Urzędzie Miasta i Gminy w Chmielniku, którego celem jest:

a) Weryfikacja poziomu spełnienia wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie KRI, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w Urzędzie Miasta i Gminy w Chmielniku,
b) Weryfikacja poziomu spełnienia wymagań pod kątem zgodności z polską normą PN-ISO/IEC 27001 lub późniejszej, w tym ocena skuteczności funkcjonujących zabezpieczeń technicznych, organizacyjnych i prawnych.
   Audyt dotyczy:
   Ilość lokalizacji: 2 lokalizacje (jedna główna i jedna zamiejscowa: 4stanowiska)
   Ilość pracowników przetwarzających dane: do 50.
   Ilość stanowisk komputerowych: do 65.
   Ilość serwerów (fizycznych i wirtualnych): 5 fizycznych, 1 wirtualny.
   Ilość systemów przetwarzających dane: 17.
   Ilość serwerowni:1 serwerownia.
   Ilość urządzeń sieciowych – (drukarki, routery, switche, przełączniki, urządzenia VoIP etc.) - drukarki-30, routery -2, switche-7, przełączniki-6, VoIP- nie ma.

Access Point: 3.
Ilość drukarek sieciowych: 10
Ilość podsieci: nie ma
Ilość adresów zewnętrznych: 3.

Audyt (przegląd i ocena) nie ma charakteru uzyskiwania certyfikatu zgodności ww. systemu zarządzania bezpieczeństwa informacji z Polską Normą PN-ISO/IEC 27001 lub późniejszą.

W postępowaniu nie mogą brać udziału podmioty, z którymi, w czasie postępowania ofertowego, Zamawiający ma podpisane klauzule lub umowy o powierzeniu danych osobowych

Termin realizacji zamówienia:

1. Audyt nr 1 w roku 2022 w październiku,

2. Audyt nr 2 w roku 2023 r. w styczniu,

Zadanie nr 4. Przeprowadzenie testów penetracyjnych systemów informatycznych JST

Ilość lokalizacji: 2 lokalizacje (jedna główna i jedna zamiejscowa: 4 stanowiska)
Ilość pracowników przetwarzających dane: do 50.
Ilość stanowisk komputerowych: do 65.
Ilość serwerów (fizycznych i wirtualnych): 5 fizycznych, 1 wirtualny.
Ilość systemów przetwarzających dane: 17.
Ilość serwerowni:1 serwerownia.
Ilość urządzeń sieciowych – (drukarki, routery, switche, przełączniki, urządzenia VoIP etc.) - drukarki-30, routery -2, switche-7, przełączniki-6, VoIP- nie ma.
Access Point: 3.
Ilość drukarek sieciowych: 10
Ilość podsieci: nie ma
Ilość adresów zewnętrznych: 3.

Zewnętrzne i wewnętrzne testy penetracyjne infrastruktury informatycznej
Testy styku sieci lokalnej z internetem przeprowadzane ze stacji roboczej podłączonej do sieci internet
Analiza topologii brzegu sieci;
Weryfikacja mechanizmów ochronnych;
Próba wykrycia usług sieciowych udostępnianych do internetu;
Detekcja wersji oraz typu oprogramowania dostępnego z sieci internet;
Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci internet;
Przedstawienie rozwiązań zwiększających bezpieczeństw styku sieci lokalnej z siecią internet.

Testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji

Analiza topologii sieci LAN;
Weryfikacja mechanizmów ochronnych w sieci;
Analiza komunikacji sieciowej;
Skanowanie portów TCP/UDP próba wykrycia usług sieciowych;
Skanowanie hostów aktywnych w sieci;
Exploitacja dostępnych urządzeń oraz usług w sieci LAN;
Przedstawienie rozwiązań zwiększających bezpieczeństw sieci LAN.

Posiadanie wersji komercyjnej oprogramowania niezbędnego do wykonania Audytu Bezpieczeństwa Sieci

W postępowaniu nie mogą brać udziału podmioty, z którymi, w czasie postępowania ofertowego, Zamawiający ma podpisane klauzule lub umowy o powierzeniu danych osobowych.

Termin realizacji zamówienia:

1. Test nr 1 w roku 2022 w październiku,

2. Test nr 2 w roku 2023 r. w styczniu,