Załącznik nr 1 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Projekt „Cyfrowa Gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego
w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020.

SPIS TREŚCI

Wstęp

Niniejszy dokument określa minimalne wymagania dla przedmiotu zamówienia dotyczącego realizacji projektu pn.: „Cyfrowa Gmina” realizowanego przez Gminę Chocz.

Zakup jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczący realizacji projektu grantowego „Cyfrowa Gmina” dla Gminy Chocz o numerze 5194.

Wymagania minimalne

Część I przedmiotu zamówienia

Serwer bazodanowy z oprogramowaniem

Nazwa	Minimalne wymagania dla sprzętu
Typ	Serwer z oprogramowaniem systemowym
Obudowa	Obudowa tower z możliwością instalacji do 4 dysków 3.5"
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Zainstalowany jeden procesor 8-rdzeniowy, min. 2.6 GHz (Turbo Speed min. 4.8 GHz), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 17550 w teście Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/.
Pamięć RAM	Minimum 2x32GB pamięci RAM ECC UDIMM o częstotliwości pracy minimum 2666MT/s. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	min. 4 porty USB w tym min. 1 USB 3.0 min. 1 port VGA min. 1 port RS232
Gniazda PCI	Min. 2 sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Kontroler dysków	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfujących.
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD, NL SAS Zainstalowane minimum 4 dyski SAS o pojemności min. 900GB, 12Gb, 15K, Hot-Plug Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Wentylatory	Minimum 3 wentylatory
Zasilacze	Zasilacz o mocy maks. 450W.
System operacyjny	Zamawiający wymaga, aby dostarczony serwer posiadał zainstalowane oprogramowanie systemowe w najnowszej aktualnej wersji,

	nieograniczonej czasowo wraz z licencją dostępową dla 20 użytkowników i licencją do pracy zdalnej dla 5 użytkowników. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 lub równoważny l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, q) wsparcie dla większości powszechnie używanych urządzeń

	peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

	2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • integracja z Active Directory; • wsparcie dla dynamic DNS;

	• wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Gwarancja	3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 lub inny równoważny oraz ISO-14001 lub inny równoważny Serwer musi posiadać deklaracja CE lub inna równoważna
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Rekonfiguracja systemów i szkolenie z dostarczonego rozwiązania	W ramach dostawy sprzętu Wykonawca zobowiązany jest do wykonania następujących usług: 1) rekonfiguracja serwera: Wykonawca stworzył plan wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający położenie Serwera Wirtualizacyjnego w szafie rack zamawiającego. · montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów. Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. · Uruchomienie systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera. · podłączenia Serwera do Przełącznika za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera · testów niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania · instalacji oprogramowania wirtualizacyjnego na dostarczonym sprzęcie

	2) szkolenie z dostarczonego rozwiązania: * szkolenie minimum 5 godzin na miejscu u Zamawiającego * zakres tematyczny: omówienie fizycznych interface'ów sprzętu - sposoby montażu w szafie RACK - sposoby podłączenia kart rozszerzeń (np. dodatkowych kart) - konfiguracja kontrolera pamięci masowej, tworzenie RAID - ustawienia BIOS - bezpieczeństwo · przeprowadzenia szkolenia z zarządzania niskopoziomowego dostarczanych serwerów obejmującą: o tworzenie grup RAID o obsługę wirtualnej konsoli (podłączanie napędów ISO) o diagnozowanie ewentualnych problemów o generowanie logów Omówienie tworzenie nowych maszyn wirtualnych oraz ich parametryzację (zarządzanie wirtualnymi kartami sieciowymi, pamięcią ram) o przedstawienie oraz charakterystyka oprogramowania do zarządzania środowiskiem wirtualizatorów o konfiguracje wirtualnej infrastruktury sieciowej (wirtualnego przełącznika) o przedstawienie i zarządzanie uprawnieniami użytkowników o usługi migawkowe dla maszyn wirtualnych o tworzenie i eksportowanie logów i konfiguracji oprogramowania wirtualizacyjnego 3) Przygotowanie niezbędnej dokumentacji w zakresie dokumentacji powdrożeniowej zawierającej opis zrekonfigurowanych opcji wdrożonego środowiska Zamawiający wymaga, aby wszystkie usługi zostały zrealizowane przez Inżyniera rozwiązania serwerowego posiadającego certyfikację producenta poświadczającą wiedzę z zakresu oferowanego sprzętu – dokumenty dołączyć do oferty.
Ilość	1 kpl.

Zasilanie awaryjne UPS

Nazwa	Minimalne wymagania dla sprzętu
Wymagania ogólne	Moc wyjściowa (pozorna): minimum 3000 VA Moc wyjściowa (czynna): minimum 3000 W Topologia: minimum VI (line interactive) Typ obudowy**:** tower Chłodzenie: Wymuszone, wewnętrzne wentylatory
Wejście	Napięcie znamionowe (wartość skuteczna): minimum 230 V AC Zakres napięcia wejściowego (wartości skuteczne) i tolerancja: minimum 178 ÷ 281 V AC ± 2 % Częstotliwość znamionowa napięcia wejściowego: minimum 50 Hz

	Zakres częstotliwości i tolerancja: minimum 45 ÷ 55 Hz ± 1 Hz Progi przełączania: sieć – UPS: minimum 178 ÷ 281 V AC ± 2 %
Wyjście	Napięcie znamionowe (wartość skuteczna): minimum 230 V AC Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa: 195 ÷ 253 V AC ± 2 % Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa: 230 V AC ± 5 % Automatyczna regulacja napięcia (AVR): ± 10 % Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej) Sinusoidalny / Tak jak na wejściu Częstotliwość znamionowa napięcia wyjściowego: 50 Hz Filtracja napięcia wyjściowego: Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy Progi przełączania: UPS – sieć: 183 ÷ 276 V AC ± 2 % Czas przełączenia na pracę rezerwową: < 3 ms Czas powrotu na pracę sieciową: 0 ms Przeciążalność: > 105% - 15 s (wyłączenie UPS)
AKUMULATORY I CZASY PODTRZYMANIA	Akumulatory wewnętrzne: minimum 12 V / 7 Ah VRLA możliwość podłączenia zewnętrznego modułu bateryjnego - wymagane Czas podtrzymania z baterii wewnętrznych lub przy wykorzystaniu zewnętrznego modułu bateryjnego (dla obciążenia 3000W) minimum 7 min Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza): do 4 h Maksymalny czas ładowania baterii wewnętrznych UPS + moduł bateryjny do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza): do 12 h
ZABEZPIECZENIA	Zabezpieczenie wejściowe: minimum - Przeciwzwarciowe – Bezpiecznik automatyczny - Przeciwprzepięciowe Zabezpieczenie wyjściowe minimum: - Elektroniczne – przeciwzwarciowe i przeciążeniowe Zabezpieczenia wejścia DC (akumulatory wewnętrzne) : Zabezpieczenie nadprądowe Zabezpieczenia DC (zewnętrzny moduł bateryjny): Zabezpieczenie nadprądowe
WYPOSAŻENIE I FUNKCJE DODATKOWE	Przyłącza wyjściowe (liczba i typ gniazd): minimum 9 gniazd z podtrzymaniem bateryjnym (w tym minimum 2 gniazda w standardzie PL z bolcem uziemiającym) Sygnalizacja: Akustyczno – optyczna; graficzny wyświetlacz LCD, Interfejsy komunikacyjne: minimum 1 x USB HID, 1 x SNMP/HTTP Filtr teleinformatyczny (linii danych) – RJ45 minimum: LAN 1 Gbit/s Wsporniki do montażu w szafie RACK Oprogramowanie monitorująco-zarządzające – wymagania minimalne: - oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS - możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP) - możliwość zdalnego wyłączenia zarządzanej sekcji gniazd - możliwość edycji nazw urządzeń na liście monitorowanych UPSów

	- wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. - wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie napięcia sieciowego Możliwość aktualizacji oprogramowania firmware przez użytkownika
Gwarancja	Min 36 miesięcy na elektronikę i 36 miesięcy na akumulatory Serwis musi być realizowany przez autoryzowany serwis producenta zlokalizowany w Polsce Serwis musi być realizowany w systemie door to door
Certyfikaty	ISO 9001:2015 lub inny równoważny dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań Certyfikat CE lub inny równoważny
Ilość	1 kpl.

Stacje robocze oprogramowaniem systemowym i monitorem

Nazwa	Minimalne wymagania dla sprzętu
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Wydajność obliczeniowa	Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 12 300 punktów według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php - wydruk należy dołączyć do oferty. Dopuszcza się wydruk w języku angielskim.
Pamięć RAM	8GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB.
Pamięć masowa	Dysk M.2 SSD 256GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”
Wydajność grafiki	Zintegrowana z procesorem
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out.
Obudowa	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 mm. Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie

	50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego

	procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi
System operacyjny	Zainstalowany system operacyjny spełniający następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Licencja bezterminowa zapewniająca prawo do wykorzystywania przez jednostki samorządu terytorialnego. 2. Polska wersja językowa. 3. System operacyjny powinien być dostarczony w najnowszej oferowanej przez producenta wersji. 4. Aktualizacje funkcji dla systemu operacyjnego. 5. Obsługa procesorów wielordzeniowych. 6. Graficzny okienkowy interfejs użytkownika. 7. Obsługa co najmniej 8 GB RAM. 8. Dostęp do aktualizacji w ramach zaoferowanej wersji systemu

	operacyjnego przez Internet bez dodatkowych opłat. 9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych: lupa powiększająca zawartość ekranu, • narrator odczytujący zawartość ekranu, • regulacja jasności i kontrastu ekranu, • możliwość odwrócenia kolorów np. biały tekst na czarnym tle, • poprawa widoczności elementów ekranu np. regulowanie grubości kursora myszy - małej strzałki na ekranie, wskazującej lokalizację myszy i czasu trwania powiadomień systemowych, • funkcja sterowania myszą z klawiatury numerycznej, • funkcja klawiszy trwałych, która sprawia, że skrót klawiszowy jest uruchamiany po naciśnięciu jednego klawisza, • korzystanie z wizualnych rozwiązań alternatywnych wobec dźwięków, • funkcja napisów w treściach wideo, • możliwość skorzystania z wizualnych rozwiązań alternatywnych wobec dźwięków; 13. Możliwość zarządzania stacją roboczą poprzez polityki. 14. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 15. Wsparcie dla min. Sun Java i .NET Framework 1.1 i 2.0 i 3.0 i 4.5 – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 16. Wsparcie dla min. JScript i VBScript - możliwość uruchamiania interpretera poleceń. 17. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 18. Graficzne środowisko instalacji i konfiguracji. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników. 20. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 21. Oprogramowanie dla tworzenia kopii zapasowych, automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 22. Możliwość przywracania plików systemowych. Możliwość identyfikacji sieci komputerowych, do których jest podłączony

	komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
Oprogramowanie biurowe	Wymagane jest dostarczenie sprzętu wraz z zainstalowanym oprogramowaniem biurowym, który musi mieć zaimplementowane co najmniej następujące funkcjonalności tj. edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej i kalendarza, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. Wymagania odnośnie interfejsu użytkownika: a) pełna polska wersja językowa interfejsu użytkownika, b) możliwość zdalnej instalacji pakietu poprzez zasady grup (GPO) w domenie, c) całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie, d) wsparcie dla formatu XML, e) możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów, f) możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony, g) możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych, w wypadku nieoczekiwanego zamknięcia aplikacji spowodowanego zanikiem prądu, h) prawidłowe odczytywanie i zapisywanie danych w dokumentach min. w formatach: .DOC, .DOCX, XLS, .XLSX, .PPT, .PPTX, w tym obsługa formatowania, makr, formuł, formularzy w tym plikach wytworzonych w MS Office 2007, MS Office 2010 i MS Office 2013, Office 2016 i) zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). Musi być kompatybilny z posiadanym przez Zamawiającego oprogramowaniem Microsoft Office i pozwalać min. na: a) otwieranie dokumentów utworzonych przy pomocy programów MS Word (od wersji 2007 do 2016), MS Excel (od wersji 2007 do 2016), MS Power Point (od wersji 2007 do 2016), b) w otwieranych dokumentach musi być zachowane oryginalne formatowanie oraz ich treść bez utraty jakichkolwiek ich parametrów i cech użytkowych (min.: korespondencja seryjna, arkusze kalkulacyjne zawierające makra i formularze.) czy też konieczności dodatkowej edycji ze strony użytkownika. Edytor tekstów musi umożliwiać min.: a) edycję i formatowanie tekstu w języku polskim wraz z obsługą

	języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, b) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), c) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, d) automatyczne tworzenie spisów treści, e) sprawdzanie pisowni w języku polskim, f) śledzenie zmian wprowadzonych przez użytkowników, g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, h) określenie układu strony (pionowa/pozioma), i) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego, j) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Arkusz kalkulacyjny musi umożliwiać min.: a) tworzenie raportów tabelarycznych, b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, d) tworzenie raportów z zewnętrznych źródeł danych (min. inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), e) tworzenie raportów tabel przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, f) wykonywanie analiz danych przy użyciu formatowania warunkowego, g) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, h) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, i) formatowanie czasu, daty i wartości finansowych z polskim formatem, j) zapis wielu arkuszy kalkulacyjnych w jednym pliku, k) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 do 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, l) zabezpieczenie dokumentów hasłem przed odczytem oraz przed

	wprowadzaniem modyfikacji. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać min. przygotowywanie prezentacji multimedialnych oraz: a) drukowanie w formacie umożliwiającym robienie notatek, b) zapisanie w postaci tylko do odczytu, c) nagrywanie narracji dołączanej do prezentacji, d) opatrywanie slajdów notatkami dla prezentera, e) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, f) tworzenie animacji obiektów i całych slajdów. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać min.: a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, c) automatyczne grupowanie poczty o tym samym tytule, d) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, e) oznaczenie poczty elektronicznej z określeniem terminu przypomnienia, f) zarządzanie kalendarzem, g) zapraszanie uczestników na spotkanie, co po ich akceptacji musi spowodować automatyczne wprowadzenie spotkania w ich kalendarzach, h) zarządzanie listą zadań, i) zlecanie zadań innym użytkownikom, j) zarządzanie listą kontaktów, k) udostępnianie listy kontaktów innym użytkownikom, l) przeglądanie listy kontaktów innych użytkowników, m) możliwość przesyłania kontaktów innym użytkowników.
Certyfikaty i standardy	• Certyfikat ISO9001 lub inny równoważny dla producenta sprzętu • Certyfikat ISO 14001 lub inny równoważny dla producenta sprzętu • Certyfikat ISO 50001 lub inny równoważny dla producenta sprzętu • Deklaracja zgodności CE lub równoważny • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych • Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym
Wymagania dodatkowe	Wbudowane porty minimum: 2x Display Port 1.4, port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu, port audio-out na tylnym panelu obudowy, 1xRJ-45, 8 portów USB wyprowadzonych na zewnątrz obudowy, w tym min 2 porty USB na przednim panelu obudowy i min. 4 porty USB 3.2 gen. 1

	Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Monitor	Typ ekranu: Ekran ciekłokrystaliczny z aktywną matrycą min. 23,8” (16:9) Technologia wykonania matrycy: IPS Jasność 250 cd/m2 Kontrast Typowy 1000:1 Kąty widzenia (pion/poziom): 178/178 stopni Czas reakcji matrycy: max. 8 ms Rozdzielczość maksymalna: 1920 x 1080 przy 60Hz Powłoka powierzchni ekranu: Antyodblaskowa utwardzona Podświetlenie: System podświetlenia LED Bezpieczeństwo: Monitor musi być wyposażony w tzw. gniazdo zabezpieczenia przed kradzieżą. Monitor musi posiadać możliwość regulowania min. kąta nachylenia oraz wysokości monitora Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie. Złącza min.: 1x D-Sub, 1x Display Port 1.2 Gwarancja: minimum 60 miesięcy, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną i stronę internetową producenta Czas reakcji serwisu - do końca następnego dnia roboczego Inne: Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub inna równoważną oraz wykazana zgodnie z normą ISO 9296 lub inną równoważną w pozycji obserwatora w trybie pracy jałowej (IDLE) wynosząca maksymalnie 26 dB (załączyć do oferty dokumenty potwierdzające).
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta

	(automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji	Minimum 36 miesięczna gwarancja producenta świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001: 2015 lub inną równoważną na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty poświadczające załączyć do oferty. Do oferty należy załączyć dokumenty poświadczające, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, producent przejmie na siebie wszelkie zobowiązania związane z serwisem. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) Zamawiający wymaga dołączenia dokumentów poświadczających, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Dodatkowe oprogramowanie	Oprogramowanie zarządzające producenta komputera, zainstalowane na etapie produkcji komputera, umożliwiające min.: - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu - powiadomienie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: -upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, -możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi, jakiego komponentu sprzętu dotyczy aktualizacja, wszystkich poprzednich aktualizacjach z

	informacjami jak powyżej. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Ilość	3 kpl.

Mobilne stacje robocze dla administratorów

Nazwa	Minimalne wymagania dla sprzętu
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Matryca	15,6" FHD (1920 x 1080), powłoka przeciwodblaskową, bez dotyku, jasność 250 cd/m2, kontrast 600:1
Procesor	Procesor osiągający w teście PassMark Performance Test, co najmniej 21 200 punktów w kategorii Average CPU Mark. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php - wydruk należy dołączyć do oferty. Dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Minimum 16GB DDR4 3200MHz możliwość rozbudowy do min. 64GB. Dwa sloty na pamięć w tym min. jeden slot wolny.
Pamięć masowa	Minimum 512GB PCIe NVMe SSD M.2
Karta graficzna	Karta graficzna zintegrowana z procesorem
Klawiatura	Klawiatura w układzie US – QWERTY z wbudowanym podświetleniem, min 78 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W. Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.

	Kamera internetowa z diodą informującą o aktywności, 0.9 Mpix, trwale zainstalowana w obudowie matrycy wyposażona w mechaniczną przysłonę. czytnik kart micro SD, 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Karta Wi-Fi 6 AX + Bluetooth 5.1
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka, po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni. Komputer spełniający normy MIL-STD-810H [załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta]
BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag z możliwością wpisywania min. znaków specjalnych. Funkcje logowania się do BIOS na podstawie hasła systemowego/użytkownika, administratora (hasła niezależne), Blokowanie hasłem systemowym/użytkownika dostępu do dysku twardego, funkcja umożliwiająca założenie hasła na dysk, informację o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS. Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym.
Certyfikaty	• Certyfikat ISO9001 lub inny równoważny dla producenta sprzętu • Certyfikat ISO 14001 lub inny równoważny dla producenta sprzętu • Certyfikat ISO 50001 lub inny równoważny dla producenta sprzętu • Deklaracja zgodności CE lub równoważny • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych • Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 23dB (załączyć do oferty dokumenty potwierdzające)
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności

	nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Wbudowany czujnik otwarcia obudowy (dolnej pokrywy) Wbudowana w obudowę matrycy technologia IR umożliwiająca autentykację na poziomie oferowanego systemu operacyjnego Czytnik linii papilarnych Czytnik SmartCard
System operacyjny	Zainstalowany system operacyjny spełniający następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Licencja bezterminowa zapewniająca prawo do wykorzystywania przez jednostki samorządu terytorialnego. 2. Polska wersja językowa. 3. System operacyjny powinien być dostarczony w najnowszej oferowanej przez producenta wersji. 4. Aktualizacje funkcji dla systemu operacyjnego. 5. Obsługa procesorów wielordzeniowych. 6. Graficzny okienkowy interfejs użytkownika. 7. Obsługa co najmniej 8 GB RAM. 8. Dostęp do aktualizacji w ramach zaoferowanej wersji systemu operacyjnego przez Internet bez dodatkowych opłat. 9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych: lupa powiększająca zawartość ekranu, • narrator odczytujący zawartość ekranu, • regulacja jasności i kontrastu ekranu, • możliwość odwrócenia kolorów np. biały tekst na czarnym tle, • poprawa widoczności elementów ekranu np. regulowanie grubości kursora myszy - małej strzałki na ekranie, wskazującej lokalizację myszy i czasu trwania powiadomień systemowych, • funkcja sterowania myszą z klawiatury numerycznej, • funkcja klawiszy trwałych, która sprawia, że skrót klawiszowy jest uruchamiany po naciśnięciu jednego klawisza, • korzystanie z wizualnych rozwiązań alternatywnych wobec dźwięków,

	• funkcja napisów w treściach wideo, • możliwość skorzystania z wizualnych rozwiązań alternatywnych wobec dźwięków; 16. Możliwość zarządzania stacją roboczą poprzez polityki. 17. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 18. Wsparcie dla min. Sun Java i .NET Framework 1.1 i 2.0 i 3.0 i 4.5 – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 19. Wsparcie dla min. JScript i VBScript - możliwość uruchamiania interpretera poleceń. 20. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 21. Graficzne środowisko instalacji i konfiguracji. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników. 23. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 24. Oprogramowanie dla tworzenia kopii zapasowych, automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania plików systemowych. Możliwość identyfikacji sieci komputerowych, do których jest podłączony komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
Oprogramowanie biurowe	Wymagane jest dostarczenie sprzętu wraz z zainstalowanym oprogramowaniem biurowym, który musi mieć zaimplementowane co najmniej następujące funkcjonalności tj. edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej i kalendarza, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. Wymagania odnośnie interfejsu użytkownika: a) pełna polska wersja językowa interfejsu użytkownika, b) możliwość zdalnej instalacji pakietu poprzez zasady grup (GPO) w domenie, c) całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie, d) wsparcie dla formatu XML, e) możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów, f) możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany

	dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony, g) możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych, w wypadku nieoczekiwanego zamknięcia aplikacji spowodowanego zanikiem prądu, h) prawidłowe odczytywanie i zapisywanie danych w dokumentach min. w formatach: .DOC, .DOCX, XLS, .XLSX, .PPT, .PPTX, w tym obsługa formatowania, makr, formuł, formularzy w tym plikach wytworzonych w MS Office 2007, MS Office 2010 i MS Office 2013, Office 2016 i) zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). Musi być kompatybilny z posiadanym przez Zamawiającego oprogramowaniem Microsoft Office i pozwalać min. na: a) otwieranie dokumentów utworzonych przy pomocy programów MS Word (od wersji 2007 do 2016), MS Excel (od wersji 2007 do 2016), MS Power Point (od wersji 2007 do 2016), b) w otwieranych dokumentach musi być zachowane oryginalne formatowanie oraz ich treść bez utraty jakichkolwiek ich parametrów i cech użytkowych (min.: korespondencja seryjna, arkusze kalkulacyjne zawierające makra i formularze.) czy też konieczności dodatkowej edycji ze strony użytkownika. Edytor tekstów musi umożliwiać min.: a) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, b) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), c) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, d) automatyczne tworzenie spisów treści, e) sprawdzanie pisowni w języku polskim, f) śledzenie zmian wprowadzonych przez użytkowników, g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, h) określenie układu strony (pionowa/pozioma), i) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego, j) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Arkusz kalkulacyjny musi umożliwiać min.: a) tworzenie raportów tabelarycznych, b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych,

	kołowych, c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, d) tworzenie raportów z zewnętrznych źródeł danych (min. inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), e) tworzenie raportów tabel przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, f) wykonywanie analiz danych przy użyciu formatowania warunkowego, g) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, h) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, i) formatowanie czasu, daty i wartości finansowych z polskim formatem, j) zapis wielu arkuszy kalkulacyjnych w jednym pliku, k) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 do 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, l) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać min. przygotowywanie prezentacji multimedialnych oraz: a) drukowanie w formacie umożliwiającym robienie notatek, b) zapisanie w postaci tylko do odczytu, c) nagrywanie narracji dołączanej do prezentacji, d) opatrywanie slajdów notatkami dla prezentera, e) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, f) tworzenie animacji obiektów i całych slajdów. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać min.: a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, c) automatyczne grupowanie poczty o tym samym tytule, d) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i

	odbiorcy, e) oznaczenie poczty elektronicznej z określeniem terminu przypomnienia, f) zarządzanie kalendarzem, g) zapraszanie uczestników na spotkanie, co po ich akceptacji musi spowodować automatyczne wprowadzenie spotkania w ich kalendarzach, h) zarządzanie listą zadań, i) zlecanie zadań innym użytkownikom, j) zarządzanie listą kontaktów, k) udostępnianie listy kontaktów innym użytkownikom, l) przeglądanie listy kontaktów innych użytkowników, m) możliwość przesyłania kontaktów innym użytkowników.
Oprogramowanie dodatkowe	Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Porty i złącza	Wbudowane porty i złącza: 1x HDMI 2.0, 2x USB 3.2 typ A, w tym 1 port

	z zasilaniem, 2x Thunderbolt 4, gniazdo linki zabezpieczającej
Warunki gwarancyjne, wsparcie techniczne	Minimum 36 miesięcy gwarancji producenta świadczonej na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) Firma serwisująca musi posiadać ISO 9001:2015 lub równoważną na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty poświadczające załączyć do oferty. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty dokumentów potwierdzających, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta
Ilość	2 kpl.

Oprogramowanie do monitorowania sieci i pracowników

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do monitorowania sieci i pracowników posiadające następujące minimalne funkcjonalności
Monitorowanie infrastruktury	Oprogramowanie musi umożliwiać minimum: Wykrywanie urządzeń w sieci poprzez skanowanie ping (oraz arp-ping). Wizualizacja stanu urządzeń w postaci ikon urządzeń na mapach sieci. Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Program powinien monitorować czas ich odpowiedzi i procent utraconych pakietów. Serwerów pocztowych: - program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę, - program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS), w razie, gdyby przestały one odpowiadać lub funkcjonowały wadliwie, - program powinien mieć możliwość wykonywania operacji testowych, - program powinien mieć możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa. Monitorowanie serwerów WWW i adresów URL. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail.

	Obsługa urządzeń SNMP wspierających SNMP v1/2/3 (przełączniki, routery, drukarki sieciowe, urządzenia VoIP). Obsługa komunikatów syslog i pułapek SNMP. Monitoring routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych, - ruchu generowanego przez podłączone stacje robocze. Wydajności systemów z rodziny Windows posiadanych przez Zamawiającego: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
Gromadzenie informacji o sprzęcie i oprogramowaniu	Oprogramowanie musi umożliwiać minimum: Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. Informacja o zainstalowanych aplikacjach oraz aktualizacjach co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. Zbieranie informacji w zakresie zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP Posiadanie możliwości wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. Możliwość odczytania numeru seryjnego (klucze licencyjne). Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. Możliwość przeglądu informacji o konfiguracji systemu, tj. komend startowy zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogra zadań.
Zdalna pomoc dla użytkowników	Oprogramowanie musi umożliwiać minimum: W ramach kontroli stacji użytkownika dostępny powinien być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. Pobieranie listy użytkowników z usługi katalogowej, Przypisywanie pracowników helpdesk do kategorii zgłoszeń. Procesowanie zgłoszeń użytkowników z wiadomości e-mail. Dołączanie załączników do zgłoszeń. Zrzuty ekranowe (podgląd pulpitu). Dystrybucję oprogramowania przez Agentów. Dystrybucję oraz uruchamianie plików za pomocą Agentów. Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku. Możliwość skonfigurowania automatyzacji procesowania zgłoszeń. Planowanie nieobecności pracowników helpdesk. Obsługę umów o gwarantowanym poziomie świadczenia usług (SLA).

	Generowanie raportów obsługi helpdesk. Zdalne wykonywanie poleceń poprzez Agentów (utworzenie / edycja konta lokalnego użytkownika systemu). Możliwość użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Oprogramowanie powinno posiadać komunikator. Oprogramowanie powinno posiadać bazę zgłoszeń umożliwiającą użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.
Aktywność użytkowników	Oprogramowanie musi umożliwiać minimum: Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach. Monitorowanie rzeczywistego użytkowania programów (procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt). Monitorowania transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika). Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen. Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Wyświetlanie statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. Wyświetlanie statystyki aktywności grupy i jej członków widoczne dla menedżera grupy. Grupowanie stron internetowych oraz aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). Przypisywanie kategorii aplikacjom i stronom internetowym, możliwość

	stworzenia predefiniowanej listy kategorii z możliwością edycji. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji.
Ochrona danych przed wyciekiem	Oprogramowanie musi umożliwiać minimum: Zarządzanie prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. Autoryzowanie urządzeń firmowych: pendrive'ów, dysków zewnętrznych - urządzenia nieautoryzowane. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Możliwość usuwania z listy znanych urządzeń tych nośników.
Licencja	Licencja powinna pozwalać na bezpłatne użytkowanie oprogramowania przez minimum 20 użytkowników wraz z suportem producenta dostępnego przez minimum 12 miesięcy.
Ilość	1 szt.

Oprogramowanie antywirusowe

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie antywirusowe do ochrony posiadanych przez Zamawiającego stacji roboczych, notebooków i serwerów
Wymagania techniczne	Dostarczone rozwiązanie musi posiadać funkcjonalności: 1. ochrona stacji roboczych w zakresie minimum: • Rozwiązanie musi wspierać systemy operacyjne Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11. • Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. • Rozwiązanie musi wspierać architekturę ARM64. • Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. • Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. • Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.

	• Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives. • Ochrona antywirusowa i antyspyware • Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. • Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. • Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. • Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. • Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. • Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu. • Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania. • Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). • Rozwiązanie musi posiadać opcję skanowania „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. • Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. • Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. • Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. • Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. • Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.

	• Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. • Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. • Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera. • W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. • Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. • Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. • Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. • Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. • Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). • Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. • Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. • Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. • Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL. • Rozwiązanie musi posiadać możliwość zdefiniowania blokady

	wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora. • Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. • Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. • Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe. • Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta. • Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego. • Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. • Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym. • Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. • W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne. • Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. • Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. • Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika. • Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni

	anonimowe. • Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. • Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. • Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło. • Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. • Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. • Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. • Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. • System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. • System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. • Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. • Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia. • Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na

automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

- Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
- Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
- W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
- Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
- Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
- Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
- Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.

	• Rozwiązanie musi posiadać zaawansowany skaner pamięci. • Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. • Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. • Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. • Rozwiązanie musi posiadać posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie. • Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. • Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. • Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji. • Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. • Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. • Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). • Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). • Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. • W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w

	harmonogramie zadań rozwiązania. • Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. • Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń. • Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji. • Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline. • Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie. • W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM. • W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. • Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej. • Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. • Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. • Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. • Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. • Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. • Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.

	• Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. • Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. • Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia. • Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup. • Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. • Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”. • Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. • Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. • Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. • Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. • Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet. • Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB. • Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. • Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu. • Ochrona przed spamem • Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. • Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. • Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy

wszystkich kontaktów z książki adresowej programu pocztowego.
- Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
- Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
- Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
- Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
- Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
- Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
- Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
- Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.
- Zapora osobista (personal firewall)
- Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
- Rozwiązanie musi oceniać reguły zapory systemu Windows.
- Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.
- Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
- Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów,

	protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego. • Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj. • Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji. • Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet. • Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu. • Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. • Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. • Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. • Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie. • Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6. • Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci. • Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: ○ z aplikacją lokalną, którą administrator wskazuje z listy, ○ z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP. ○ Kontrola dostępu do stron internetowych • Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

	• Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory. • Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. • Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. • Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych. • Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta. • Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. • Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj. • Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej. • Bezpieczna przeglądarka • Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. • Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. • Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki. • Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę. • Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki. • Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce

przeglądarki.

2. Ochrona serwerów w zakresie minimum:
   - Rozwiązanie musi posiadać wsparcie dla systemów Microsoft Windows Server 2008 R2 i nowszych.
   - Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
   - Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
   - Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
   - Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
   - Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
   - Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
   - Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu.
   - Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
   - Rozwiązanie musi posiadać opcję skanowania „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
   - Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
   - Rozwiązanie ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
   - Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
   - Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
   - Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
   - Rozwiązanie musi wspierać mechanizm klastrowania.
   - Rozwiązanie musi być wyposażone w system zapobiegania

	włamaniom działający na hoście (HIPS). ● Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: ○ tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, ○ tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, ○ tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, ○ tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, ○ tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. ● Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. ● Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. ● Rozwiązanie musi posiadać zaawansowany skaner pamięci. ● Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. ● Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS. ● Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze. ● Rozwiązanie musi umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. ● Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych

	urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. • Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. • Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia. • Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. • Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. • W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. • Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. • Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. • Dodanie automatycznych wyłączeń nie wymaga restartu serwera. • Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. • Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. • Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. • Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). • Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. • Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne

	oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. • Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. • Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. • Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. • Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. • W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. • Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. • Rozwiązanie musi posiadać możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło. • Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. • Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji. • Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje • krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. • Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. • System antywirusowy, uruchomiony z płyty bootowalnej lub

	pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. • System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. • Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. • Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. • Rozwiązanie musi oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. • Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. • Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. • Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. • Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. • Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. • Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). • Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). • Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. • Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. • Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych

	aktualizacji modułów i samego oprogramowania. • Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść". • Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. • Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia. • Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. • Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. • Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet. • Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. • Rozwiązanie musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów. • Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. • Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. • Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. • Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 3. Możliwość administracji zdalnej w zakresie minimum: • Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux. • Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.

	• Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. • Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik. • Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. • Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. • Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. • Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy. • Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6. • 10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs. • Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji. • Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. • Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym. • Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. • Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. • Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. • Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”. • Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów. • Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy. • Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. • Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.

	• Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS. • Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP. • Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11. • Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap. • Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych. • Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów. • Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. • Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. • Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android. • Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS. • Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci. • Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. • Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające. • Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor,

	pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania. • Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. • Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny. • W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play. • Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. • Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS. • Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego. • Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi. • Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. • Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. • Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. • Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej. • Serwer administracyjny musi posiadać możliwość konfiguracji

	czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany. • Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. • Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. • Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych. • Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. • Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej. • Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. • Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. • Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. • Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania. • Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. • Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta. • Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.

	• Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji. • Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce. • Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta. • Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów. • Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie. • Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy. • Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania. • Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów. • Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny. • Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może • zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV. • Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. • Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów. • Powiadomienia mailowe mają być wysyłane w formacie HTML. • Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń. • Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. • Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez

	administratora okresie czasu. • Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji. • Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami. • Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych. • W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu. • Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. • Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan. • Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. • Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli. • W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych. • Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta. • Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli. • Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania. • Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie. • Konsola administracyjna musi umożliwiać personalizację interfejsu webowego. • Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych. • Konsola administracyjna musi mieć możliwość zarządzania

	rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault). • Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk. • Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal). • Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów. 5. Sandboxing w chmurze w zakresie minimum: • Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. • Rozwiązanie musi wykorzystywać do działania chmurę producenta. • Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. • Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. • Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. • Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. • Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. • Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. • Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. • Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. • Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do

analizy oraz przez kogo.
- Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
  - Czysty,
  - Podejrzany,
  - Bardzo podejrzany,
  - Szkodliwy.
- W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
- W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

6. Szyfrowanie w zakresie minimum:
- System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
- System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
- Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
- Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
- Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
- Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.
- Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
- W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.
- Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.
- Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku

	ratunkowego. • Musi istnieć możliwość konfiguracji złożoności hasła 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. • Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom. • Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.
Licencja	Licencja powinna pozwalać na bezpłatne użytkowanie oprogramowania przez minimum 26 użytkowników wraz z suportem producenta dostępnego przez minimum 12 miesięcy.
Ilość	1 kpl.

Oprogramowanie do backupu

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do backupu
Wymagania ogólne	1) Oprogramowanie może być dostarczane w dwóch scenariuszach: - Cloud (Software as Service), - On-premise. 2) Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-pr oraz cloud. 3) Interfejs systemu dostępny jest w języku: - polskim, - angielskim. 4) Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowan konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych, 5) Oprogramowanie może być uruchomione w kontenerze docker, 6) Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych systemy minimum: - Debian: 9+ - Ubuntu: 16.04+ - Fedora: 29+ - centOS: 7+ - RHEL: 6+

	- openSUSE: 15+ - SUSE Enterprise Linux (SLES): 12 SP2+ - Windows Client: 7, 8.1, 10 (1607+) - Windows Server: 2008 R2+. 7) System wykonuje kopię własnej bazy danych, która umożliwia odtworze wszystkich ustawień i całej konfiguracji, 8) Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju).
Zarządzanie	1) Zarządzanie całością działania systemu (backup, przywracanie) z poziom jednej konsoli webowej, 2) Zarządzanie całym systemem poprzez dashboardy, 3) Gradacja uprawnień kont administratorów z poziomu panelu zarządzając 4) System posiada wbudowane predefiniowane zadania backupowe, 5) System umożliwia tworzenie zadań backupowych w oparciu o kalendarz. 6) Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem, 7) Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie ustalonym harmonogramem, 8) Monitorowanie postępu działania zadania, 9) Posiada system powiadamiania poprzez e-mail o zdarzeniach w następuj przypadkach: - Zadanie zostało zakończone pomyślnie, - Zadanie zostało zakończone z ostrzeżeniami, - Zadanie zostało zakończone z błędem, - Zadanie zostało anulowane, - Zadanie nie zostało uruchomione. 10) System generuje alerty na konsoli WEB w przypadku zaistnienia określo zdarzenia systemowego. 11) Możliwość zdefiniowania okna backupowego dla każdego z zadań, 12) Oprogramowanie posiada wbudowany menadżer haseł do przechowywa kluczy szyfrujących oraz poświadczeń do magazynów, 13) System pozwala na klonowanie planów kopii zapasowych, 14) System umożliwia reset hasła administratora w przypadku jego utraty, 15) Oprogramowanie umożliwia definiowanie retencji według schematów: GFS(Grandfather-Father-Son), FIFO(First-In, First-Out). 16) Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami, 17) Konta użytkowników mogą być tworzone poprzez import pliku CSV, 18) Oprogramowanie umożliwia tworzenie grup urządzeń, 19) Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych po możliwość wybrania dowolnego workera(urządzenia, które odpowiadać b za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, k będzie wykorzystywane do przeszukiwania m.in. magazynów). 20) System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak in.: - System Administrator, - Backup operator, - Restore operator,

	- Viewer.
Składowanie danych	1) Oprogramowanie jest systemem multi-storageowym i umożliwia tworzer wielu repozytoriów danych jednocześnie, 2) System umożliwia składowanie danych: a) Lokalnie: - Zasób SMB, - Zasób NFS, - Zasób ISCSI, - Zasób S3, - Katalog zabezpieczonego urządzenia. b) W chmurze: - Amazon Web Service, - Magazyn zgodny z S3, - Dostarczanej przez producenta. 3) System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji, 4) System oferuje mechanizm składowania kopii backupowych (retencja da w nieskończoność lub oparty o czas i cykle.
Odtwarzanie	1) Odtwarzanie granularne: - Pojedynczych plików z kopii obrazu dysku, - Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365, 2) Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całe dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania syste awarii, wsparcie dostępne jest dla systemów: - Windows: 7+, - Windows Server: 2008 R2+, 3) Odtwarzanie Bare metal Restore może odbywać się na takim samym spr jak ten który był backupowany, jak również na zupełnie innym kompute serwerze z automatycznym dopasowaniem sterowników oraz z możliwoś dodania sterowników przez użytkownika. 4) Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej pły lub pendrive'a, 5) Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, V2P, V2V. 6) Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranyr formacie (VHD, VHDX, VMDK), 7) Odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL), 8) Odtwarzanie zasobów plikowych z prawami dostępu, 9) Przywracanie plików pomiędzy systemami operacyjnymi (np. odtwarzani danych plikowych Linux na systemie Windows), 10) Odtwarzanie danych według harmonogramu, 11) Przywracanie danych z określonego urządzenia/użytkownika, 12) Przywracanie kopii z wybranego magazynu. 13) Przywracanie danych Microsoft 365: a) do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w form pliku: - pst, - mbox. b) do istniejącego konta w usłudze Microsoft 365 (tego samego lub inn tym w innej organizacji),

	14) System posiada możliwość nieodwracalnego kasowania danych, 15) Przywracanie repozytoriów GIT: - Przywracanie pomiędzy hostingami repozytoriów (GitHub/BitBucket), - przywracanie między kontami.
Backup	1) Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a backupu syntetycznego dla: A) Systemów operacyjnych: - Alpine 3.10+, - Debian: 9+, - Ubuntu: 16.04+, - Fedora: 29+, - centOS: 7+, - RHEL: 6+, - openSUSE: 15+, - SUSE Enterprise Linux (SLES): 12 SP2+, - macOS: 10.13+, - Windows: 7, 8.1, 10(1607+), - Windows Server: 2008 R2+, b) Środowisk wirtualnych: - Hyper-V, - VMware: 6.7+. c) Repozytoriów GIT: - GitHub, - Bitbucket. 2) Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla: a) Baz danych: - Microsoft SQL, - MySQL, - PostgreSQL, - Firebird, - Dowolnych innych przez podpięcie skryptów pre/post. 3) Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości: - 128 bit, - 192 bit, - 256 bit. 4) Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: - ZStandard, - LZ4. 5) Oprogramowanie umożliwia zarządzanie poziomem kompresji, 6) Wykonywanie kopii zapasowej otwartych plików (VSS), 7) System umożliwia uruchamianie skryptów przed i po backupie, 8) System umożliwia uruchamianie skryptów po wykonaniu migawki VSS, 9) System umożliwia automatyczne ponawianie prób utworzenia kopii zapa w przypadku błędów, 10) Backup jednego oraz wielu dysków/całego systemu operacyjnego (Wind ze wsparciem dla partycji MBR oraz GPT, 11) Backup plikowy,

	12) Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe, 13) Oprogramowanie umożliwia konsolidację wersji kopii zapasowych, 14) Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypa wymagania granularnego odtworzenia, 15) Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasow podczas zamykania systemu operacyjnego. 16) Oprogramowanie pozwala na backup zaszyfrowanych partycji.
Wsparcie techniczne	1) Pomoc techniczna w językach minimum: - polskim, - angielskim. 2) Materiały samopomocowe minimum: a) Baza wiedzy: - polski, - angielski
Licencjonowanie	1) Sposób licencjonowania opiera się na: - Ilości serwerów/endpointów- dla fizycznych urządzeń, - Ilości fizycznych hostów - dla środowisk wirtualnych, - Ilości repozytoriów - dla GIT. 2) Licencje powinny pozwalać na zabezpieczenie: - 20 stacji roboczych w opcji dożywotniej, - Nielimitowanej ilości maszyn wirtualnych w obrębie 2 fizycznych serwe stanowiących podstawy do wirtualizacji (Bez limitu socketów oraz procesorów). 3) Wsparcie techniczne: - Świadczone jest w języku polskim, bezpośrednio przez główną siedzibe producenta, - Zapewnia dostęp do aktualizacji oprogramowania, - Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, - Obowiązuje przez okres minimum 12 miesięcy.
Ilość	1 kpl.

Urządzenie do backupu

Nazwa	Minimalne wymagania dla usługi
Typ	Urządzenie do backupu spełniające wymagania minimalne
Wymagania sprzętowe	Procesor: Architektura 64 bit Procesor liczba rdzeni: Nie mniej niż 4 Pamięć RAM: Nie mniej niż 4GB DDR4 Pamięć RAM liczba slotów: Minimum 1 slot Pamięć RAM: możliwość rozszerzenia nie mniej niż do 16GB Pamięć Flash: Nie mniej niż 512MB Liczba zatok na dyski twarde: Minimum 8 Obsługiwane dyski twarde: 3.5" oraz 2.5" SATA Pojemność możliwych do stosowania dysków twardych: do 18TB Możliwość podłączenia modułu rozszerzającego: Tak, co najmniej dwóch

	Porty LAN: Minimum 2 x 2,5 Gb/s lub 4 x 1 Gb/s Porty LAN 10 Gb/s: Minimum 2 na złączu SFP+ Diody LED: Minimum Status, LAN, HDD, Porty USB 3.2: Minimum 4 Port PCiE umożliwiające rozbudowę urządzenia o dodatkowe karty rozszerzeń: Minimum 1 Przyciski: minimum reset, zasilanie Typ obudowy: RACK, maksymalnie 2U Zasilanie: Zasilacz 250 W, 100-240 V
Dołączone dyski do urządzenia	Minimum 4 szt. X 2 TB Kompatybilne z dostarczonym rozwiązaniem
Wymagania dla oprogramowania	Agregacja łączy Obsługiwane systemy plików: - Dyski wewnętrzne: EXT4 - Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ Możliwość podłączenia karty WLAN na USB Szyfrowanie wolumenów: minimum AES 256 Szyfrowanie dysków zewnętrznych Zarządzanie dyskami: - Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, - Obsługa Hot Spare per grupa RAID oraz global hot spare - Rozszerzanie pojemności Online RAID - Migracja poziomów Online RAID - HDD S.M.A.R.T. - Skanowanie uszkodzonych bloków (pliku) - Przywracanie macierzy RAID - Obsługa map bitowych - Pula pamięci masowej - Obsługa migawek woluminów i LUN blokowych - Obsługa replikacji migawek Wbudowana obsługa iSCSI : - Multi-LUN na Target - Obsługa LUN Mapping & Masking - Obsługa SPC-3 Persistent Reservation - Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN Zarządzanie prawami dostępu: - Ograniczenie dostępnej pojemności dysku dla użytkownika - Importowanie listy użytkowników - Zarządzanie kontami użytkowników - Zarządzanie grupą użytkowników - Zarządzanie współdzieleniem w sieci - Tworzenie użytkowników za pomocą makr - Obsługa zaawansowanych uprawnień dla podfolderów, - Windows ACL Obsługa Windows AD: - Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web - Funkcja serwera LDAP Funkcje backup: - Oprogramowanie do tworzenia kopii bezpieczeństwa producenta

	urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, Współpraca z zewnętrznymi dostawcami usług chmury: - Google Drive - Dropbox - Microsoft OneDrive - Microsoft OneDrive for Business i Box Darmowe aplikacje na urządzenia mobilne: - Monitoring i zarządzanie urządzeniem - Synchronizacja plików - Obsługa kamer - Dostępne na systemy iOS oraz Android Minimum obsługiwane serwery: - Serwer plików - Serwer FTP - Serwer WEB - Serwer kopii zapasowych - Serwer multimediów UPnP - Serwer pobierania (Bittorrent / HTTP / FTP) - Serwer Monitoringu VPN: - VPN client / VPN server - Obsługa PPTP - OpenVPN Administracja systemu: - Połączenia HTTP/HTTPS - Powiadamianie przez e-mail (uwierzytelnianie SMTP) - Powiadamianie przez SMS - Ustawienia inteligentnego chłodzenia - DDNS oraz zdalny dostęp w chmurze - SNMP (v2 & v3) - Obsługa UPS z zarządzaniem SNMP (USB) - Obsługa sieciowej jednostki UPS - Monitor zasobów - Kosz sieciowy dla CIFS/SMB oraz AFP - Monitor zasobów systemu w czasie rzeczywistym - Rejestr zdarzeń - System plików dziennika - Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line - Aktualizacja oprogramowania - Ustawienia: Back up, przywracania, resetowania systemu Konteneryzacja: możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker Zabezpieczenia: - Filtracja IP - Ochrona dostępu do sieci z automatycznym blokowaniem oraz blokowanie na podstawie Geolokalizacji - Połączenie HTTPS - FTP z SSL/TLS (Explicit) - Obsługa SFTP (tylko admin)

	- Szyfrowanie AES 256-bit - Szyfrowana zdalna replikacja (Rsync poprzez SSH) - Import certyfikatu SSL - Powiadomienia o zdarzeniach za pośrednictwem Email i SMS" - Możliwość instalacji dodatkowego oprogramowania Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	Minimum 36 miesięcy
Ilość	1 kpl.

Urządzenie klasy UTM z niezbędnymi serwisami i aktualizacjami

Nazwa	Minimalne wymagania dla sprzętu
Typ	Urządzenie klasy UTM wraz z niezbędnymi serwisami i aktualizacjami oraz wdrożeniem i szkoleniem
Wymagania techniczne	Dostarczone urządzenie klasy UTM musi posiadać następujące minimalne funkcje: 1. Obsługa sieci w zakresie minimum: Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. 2. Zapora korporacyjna (Firewall) w zakresie minimum: ● Urządzenie musi być wyposażone w Firewall klasy Stateful Inspection. ● Urządzenie musi obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. ● Urządzenie musi dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). ● Interface (GUI) do konfiguracji firewall musi umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca musi mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. ● Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. ● Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. ● Administrator musi mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł

	firewall. ● Edytor reguł firewall musi posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). ● Firewall musi umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). 3. INTRUSION PREVENTION SYSTEM (IPS) w zakresie minimum: ● System detekcji i prewencji włamań (IPS) musi być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. ● Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. ● Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. ● Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. ● Moduł IPS musi nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. ● Urządzenie musi mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. ● Administrator urządzenia musi mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. ● Urządzenie musi mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 4. Kształtowanie pasma (Traffic Shapping) w zakresie minimum: ● Urządzenie musi mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. ● Ograniczenie pasma lub priorytetyzacja musi być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. ● Rozwiązanie musi umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). ● Urządzenie musi umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. 5. Ochrona antywirusowa – wymagania minimalne: ● Rozwiązanie musi pozwalać na zastosowanie jednego z co

najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
- Co najmniej jeden z dwóch skanerów antywirusowych musi być dostarczany w ramach podstawowej licencji.
- Administrator musi mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
- Administrator musi mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto musi być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

6. Ochrona antyspam – wymagania minimalne:
   - Producent musi udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
   - Ochrona antyspam musi działać w oparciu o:
     a. białe/czarne listy,
     b. DNS RBL,
     c. heurystyczny skaner.
   - W przypadku ochrony w oparciu o DNS RBL administrator musi mieć możliwość modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
   - Wpis w nagłówku wiadomości zaklasyfikowanej jako spam musi być w formacie zgodnym z formatem programu Spamassassin.
7. Wirtualne sieci prywante (VPN) – wymagania minimalne:
   - Urządzenie musi posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
   - Odpowiednio kanały VPN można budować w oparciu o:
     a. PPTP VPN,
     b. IPSec VPN,
     c. SSL VPN.
   - SSL VPN musi działać w trybach Tunel i Portal.
   - W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
   - Urządzenie musi posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
   - Urządzenie musi posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
   - Urządzenie musi umożliwiać tworzenie tuneli w oparciu o technologię Route Based.
8. Filtr dostępu do stron www – wymagania minimalne:
   - Urządzenie musi posiadać wbudowany filtr URL.
   - Filtr URL musi działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron

	internetowych. ● Administrator musi mieć możliwość dodawania własnych kategorii URL. ● Urządzenie nie może być limitowane pod względem kategorii URL dodawanych przez administratora. ● Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. ● Administrator musi posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. ● Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. ● Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. ● Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. ● Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. ● Urządzenie musi posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 9. Uwierzytelnianie – wymagania minimalne: ● Urządzenie musi zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. ● Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. ● Rozwiązanie musi zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. ● Urządzenie musi posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. ● Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. ● Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. 10. Administracja łączami do internetu (ISP) – wymagania minimalne: ● Urządzenie musi posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

	• Mechanizm równoważenia obciążenia łącza internetowego musi działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. • Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. • Urządzenie musi posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. • Urządzenie musi posiadać mechanizm statycznego trasowania pakietów. • Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. • Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. • Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 11. Pozostałe usługi i funkcje rozwiązania: • Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. • Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. • Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. • Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS. • Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. • Urządzenie musi posiadać usługę DNS Proxy. 12. Administracja urządzeniem – wymagania minimalne: • Konfiguracja urządzenia musi być możliwa z wykorzystaniem polskiego interfejsu graficznego. • Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. • Komunikacja może odbywać się na porcie innym niż https (443 TCP). • Urządzenie musi być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. • Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.

	• Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. • Urządzenie musi mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). • Rozwiązanie musi mieć możliwość eksportowania logów za pomocą protokołu IPFIX. • Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. • Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. • Urządzenie musi posiadać funkcjonalność anonimizacji logów. • Urządzenie musi mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów. • Urządzenie musi mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów • Wraz z urządzeniem musi zostać dostarczona kompatybilna z urządzeniem klasy UTM, karta pamięci typu SD o pojemności minimum 128GB, o klasie prędkości minimum 10. 13. Raportowanie – wymagania minimalne: • Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. • System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. • System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. • System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. • System raportujący musi dawać możliwość edycji konfiguracji z poziomu raportu. • W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. • Dodatkowy system musi umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy. 14. Parametry sprzętowe – wymagania minimalne: • Urządzenie musi być pozbawione dysku twardego, a

	oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. ● Liczba portów Ethernet 10/100/1000Mbps – min.8. ● Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. ● Przepustowość Firewall – min. 2 Gbps. ● Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – min. 1.6 Gbps. ● Przepustowość filtrowania Antywirusowego – min. 400 Mbps. ● Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 350 Mbps. ● Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 50. ● Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. ● Obsługa min. VLAN 64. ● Liczba równoczesnych sesji - min. 200 000 i nie mniej niż 15000 nowych sesji/sekundę. ● Urządzenie nie może być nielimitowane na użytkowników. ● Urządzenie musi mieć możliwość utworzenia 4096 reguł filtrowania. ● Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów.
Gwarancja	Wymaga się, aby dostawa obejmowała również minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu oraz licencje dla wszystkich funkcji bezpieczeństwa.
Wymagania dodatkowe	Wymagane jest dostarczenie wraz z urządzeniem klasy UTM półki do szafy rackowej „19” W ramach dostawy Wykonawca zobowiązany jest do przeprowadzenia: 1) Wdrożenie -Wstępna konfiguracja urządzenia (zaadresowanie interface'ów, konfiguracja routingu, DNS, NTP), -Konfiguracja profilów administracyjnych, Podpięcie weryfikacja statusu licencji, -Konfiguracja obiektów adresowych na potrzeby polityk Firewall (na podstawie przygotowanej wcześniej listy), -Konfiguracja polityk Firewall pomiędzy strefami bezpieczeństwa, -Weryfikacja komunikacji pomiędzy strefami bezpieczeństwa, -Konfiguracja lokalnej bazy użytkowników oraz zdefiniowanie grup, oraz podłączenie do usługi LDAP/AD Konfiguracja VPN wg potrzeby -Konfiguracja IPSec VPN site-to-site, --Konfiguracja IPSec VPN client-to-site, -Konfiguracja SSL VPN client-to-site, -Konfiguracja profilów kontroli Antywirusowej i podpięcie do polityk FW, -Konfiguracja profilów ochrony przed atakami IPS i podpięcie do polityk FW, -Konfiguracja profilów kontroli aplikacji i podpięcie do polityk FW, -Konfiguracja profilów kontroli WWW i podpięcie do polityk FW,

	-Konfiguracja profilów antyspamowych i podpięcie do polityk FW, -Test zastosowanych funkcji ochronnych, -Przygotowania ogólnej dokumentacji z zakresu zdefiniowanych funkcji. 2) Instruktaż zdalny Wymagane jest, aby wdrożenie oraz instruktaż został wykonany przez inżynierów certyfikowanych przez producenta dostarczonego rozwiązania klasy UTM (do oferty dołączyć certyfikaty inżynierów) w minimalnym zakresie: -Przeszkolenie z zakresu zarządzania wszystkimi elementami podlegającymi konfiguracji w punkcie "Wdrożenie" -Szkolenie musi trwać minimum 3h -Szkolenie z odtwarzania konfiguracji po awarii urządzenia backup lokalny/backup z chmury producenta. -Przeszkolenie z zakresu prostych narzędzi do rozwiązywania problemów.
Ilość	1 szt.

Część II przedmiotu zamówienia

Audyt cyberbezpieczeństwa

Nazwa	Minimalne wymagania dla usługi
Typ	Wykonanie audytu diagnozy cyberbezpieczeństwa, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do dokumentacji konkursowej - Cyfrowa Gmina. Diagnoza cyberbezpieczeństwa powinna zostać przeprowadzona w terminie do 3 miesięcy od podpisania umowy. Wynikiem przeprowadzenia diagnozy musi być raport dotyczący audytowanego środowiska oraz wypełnienie formularza diagnozy i dostarczenia go za pomocą elektronicznej skrzynki podawczej ePUAP do NASK na adres skrzynki: /NASK-Instytut/SkrytkaESP.
Plan audytu	Audyt musi składać się z minimum: 1. Audyt dokumentacji i procesów: - ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC) - ocena wybranych aspektów bezpieczeństwa systemów informatycznych - ocena dojrzałości wybranych procesów bezpieczeństwa - opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny 2. Testy penetracyjne infrastruktury sieciowej - Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci - skanowanie sieci, rekonesans sieci (skanowanie musi zostać powtórzone dla każdej wskazanej przez Zamawiającego sieci) - skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), który zostały wybrane na podstawie wcześniejszej analizy - sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy - sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł - weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych - weryfikacja zabezpieczeń urządzeń sieciowych - testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej - wykonanie raportu zawierającego minimum: ● opis wszystkich elementów, które zostały poddane audytowi ● podział podatności ze względu na ryzyko: wysoki, średni, niski ● wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności ● wylistowanie wszystkich podatności ze względu na ryzyko: wysoki, średni, niski ● określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności - Wsparcie poaudytowe - Udzielenie informacji na temat audytowanych elementów wynikających z raportu. Czas dla klienta na zapoznanie się z raportem i zadawanie pytań odnośnie raportu.

Wymagania dla audytora	Audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu: 1. Certified Internal Auditor (CIA). 2. Certified Information System Auditor (CISA); 3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób; 4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób; 5. Certified Information Security Manager (CISM). 6. Certified in Risk and Information Systems Control (CRISC). 7. Certified in the Governance of Enterprise IT (CGEIT). 8. Certified Information Systems Security Professional (CISSP). 9. Systems Security Certified Practitioner (SSCP). 10. Certified Reliability Professional; 11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

Wymagania dodatkowe

W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do dostawy przedmiotu zamówienia wraz z jego rozpakowaniem, sprawdzeniem poprawności działania i ustawieniem w wyznaczonym przez Zamawiającego pomieszczeniu na terenie Urzędu.

Wykonawca zobowiązany do utylizacji na własny koszt wszelkich niepotrzebnych materiałów zabezpieczających urządzenia podczas transportu, w tym kartony, folie, taśmy klejące etc.

Wykonawca zobowiązany jest do ustalenia terminów dostaw z Zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Urzędu.