Załącznik nr 5 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

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

SPIS TREŚCI

Wstęp 3

Część I Przedmiotu zamówienia 3

Serwer domenowy z system operacyjnym ... 3
Modernizacja dostarczanego sprzętu serwerowego ... 7
Przełączniki zarządzalne ... 7
Stacje robocze z oprogramowaniem ... 9
Mobilna stacja robocza z oprogramowaniem ... 15
Urządzenie wielofunkcyjne A0 ... 18
Oprogramowanie do monitorowania sieci i pracowników ... 19
Oprogramowanie do backupu stacji roboczych ... 20
Urządzenia do backupu - typ I ... 20
Urządzenia do backupu - typ II ... 23
Urządzenia do backupu - typ III ... 25

Część II Przedmiotu zamówienia 27

Certyfikowane szkolenie dla administratora z dostarczonych rozwiązań oraz z zakresu cyberbezpieczeństwa ... 27
Szkolenia dla pracowników z zakresu cyberbezpieczeństwa oraz dostarczonego oprogramowania ... 42

Część III Przedmiotu zamówienia 46

Diagnoza cyberbezpieczeństwa ... 46

Wstęp

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

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 Świebodzin.

Zamówienie zostało podzielone na trzy części:

- CZEŚĆ I - Dostawa sprzętu komputerowego
- CZĘŚĆ II –Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa
- CZĘŚĆ III - Wykonanie audytu diagnozy cyberbezpieczeństwa

Wymagania minimalne

Część I – Dostawa sprzętu komputerowego

Serwer domenowy z system operacyjnym

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i odpowiednio oznaczona (np. jego znakiem firmowym).
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Jeden procesor 6-rdzeniowy, umożliwiający osiągnięcie wyniku min. 55.5 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org (https://www.spec.org/cpu2017/results/rint2017.html) w konfiguracji jednoprocesorowej. Weryfikacja zostanie przeprowadzona po upływie terminu składania ofert, co oznacza, że jeśli wynik zostanie osiągnięty do upływu terminu składania ofert, wówczas możliwe będzie potwierdzenie uzyskania wymaganego minimalnego wyniku.
Pamięć RAM	2x16GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/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. 1920x1200
Wbudowane porty	min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, min. 1 port RS232
Gniazda PCI	Min. 3 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, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.

Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD, NL SAS Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB, 6Gb, Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
System operacyjny/dodatkowe oprogramowanie	Zamawiający wymaga, aby dostarczony serwer posiadał zainstalowane oprogramowanie systemowe w najnowszej aktualnej wersji, nieograniczonej czasowo wraz z licencją dostępową dla 110 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.
Diagnostyka	Możliwość wyposażenia w panel umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Wentylatory	Minimum 4 wentylatory
Zasilacze	Redundantne, o mocy maks. 600W.
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
Diagnostyka	Możliwość wyposażenia w panel 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); - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - wsparcie dla: o IPv6; o WSMAN (Web Service for Management); o SNMP; o IPMI2.0, o SSH, o Redfish; - dynamic DNS;
Gwarancja	Minimum 36 miesięcy gwarancji, z czasem reakcji do następnego dnia roboczego od dnia przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną prowadzoną w języku polskim Zamawiający wymaga aby w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego. Możliwość sprawdzenia statusu gwarancji.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 lub normą równoważną oraz ISO-14001 lub normą równoważną. Serwer musi posiadać deklarację CE.
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Wdrożenie	W ramach dostawy sprzętu Wykonawca zobowiązany jest do wykonania następujących usług: 1) rekonfiguracja serwera: -Wykonawca stworzy plan wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający położenie Serwera Wirtualizacyjnego w szafie rack zamawiającego. - Wykonawca dokona 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. - Wykonawca uruchomi systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera. Wykonawca dokonapodłączenia Serwera do Przełącznika za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera Wykonawca wykona testy niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania Wykonawca dokona 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 Wymaga się aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta. 4) Wymaga się, aby Dostawca serwera z systemem operacyjnym zapewnił dostęp do urządzenia kryptograficznego spełniającego wymagania FIPS-140 Level minimum 3. Urządzenie to może być dostępne dla Zamawiającego jako urządzenie w Cloud z gwarancją przechowywania kluczy kryptograficznych na terenie Polski, lub jako osobne urządzenie w formie karty PCIe lub osobnego urządzenia dostępnego z poziomu sieci LAN. Na potrzeby udostępnienia takiej usługi Wykonawca musi zapewnić osobny slot urządzenia kryptograficznego na wyłączne potrzeby Zamawiającego. Wymagane interfejsy komunikacji z urządzeniem kryptograficznym PKCS#11, CSP/CNG. Komunikacja sieciowa pomiędzy siedzibą Zamawiającego a urządzeniem kryptograficznym musi być zaszyfrowana za pomocą połączenia IPSEC z kluczem szyfrującym o długości minimum 256bitów typu AES. Dopuszczalne jest użycie algorytmu ECC o długości 192bitów.
Ilość	1 kpl.

Modernizacja dostarczanego sprzętu serwerowego

Nazwa	Minimalne wymagania dla usługi
Typ	Rozbudowa posiadanej infrastruktury serwerowej
Wymagania minimalne	W ramach dostawy Wykonawca zobowiązany jest do przeprowadzenia rozbudowy dostarczanego serwera domenowego z systemem operacyjnym w zakresie minimalnym: a) Pamięć masowa: minimum 4 x 480GB SSD SATA Read Intensive 6Gbps 512 2,5in Hot-Plug AG Drive (RAID 10) b) Pamięć masowa: minimum 2 x Dyski M2 min 256GB c) Pamięć RAM: minimum 2 x 16GB UDIMM, 3200MT/s, ECC wraz z usługą instalacji w siedzibie Zamawiającego.
Ilość	1 kpl.

Przełączniki zarządzalne

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia.
Porty	Minimum 48 porty 10/100/1000Mbps RJ45, minimum 2 porty SFP/SFP+ 1/10GbE, 1 port konsolowy Obsługa modułów SFP: 1000BASE Obsługa modułów SFP+: 10GbE, SR, LR, ER

Wydajność przełącznika	Minimum 8000 adresów MAC Prędkość robocza min. 100Gbps Szybkość przełączenia min. 100Mpps Pamięć flash min. 128MB
Funkcjonalność warstwy II	Obsługa minimum 256 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa 16 grup LACP i 8 portów fizycznych per grupa Obsługa technologii port mirroring oraz remote port mirroring Obsługa funkcjonalności Voice VLAN
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego IPv4 Obsługa minimum 64 wpisów routingu dynamicznego IPv4 Obsługa protokołu RIP2
Inne Funkcjonalności	Możliwość połączenia w stos do 4 urządzeń tego samego typu Wydajność połączenia pomiędzy przełącznikami w stosie min. 20Gbps Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) on Management Ports 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIv2 1908 Coexistence Between SNMPv1/v2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2096 IP Forwarding Table MIB 2233 Interfaces Group using SMIv2 2246 TLS v1 2271 SNMP Framework MIB 2618 RADIUS Authentication MIB 2620 RADIUS Accounting MIB 2819 RMON MIB (groups 1, 2, 3, 9)

	2863 Interfaces MIB 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 3410 Internet Standard Mgmt. Framework 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3418 SNMP MIB 3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia.
Wdrożenie	W ramach dostawy sprzętu Wykonawca zobowiązany jest także do przeprowadzenia wdrożenia dostarczanego przełącznika, które musi objąć zakres minimum: - fizyczny montaż i adresację - konfiguracje do 5 wirtualnych sieci (VLAN). - segmentację sieci z podziałem na sieć do zarządzania oraz sieć lan - wykonanie jednej spójnej dokumentacji sieci w wdrażanego urządzenia (urządzeń sieciowych) w ramach całego postępowania.
Ilość	4 szt.

Stacje robocze z oprogramowaniem

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.
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark wg stanu na dzień 4 października 2022 r., w kategorii Average CPU Mark wynik co najmniej 20 300 pkt. Według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php.
Pamięć RAM	8GB DDR4 3200MHz, możliwość rozbudowy do min 64GB, minimum jeden slot DIMM wolny.
Pamięć masowa	Min. 256GB SSD PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”.
Karta graficzna	Zintegrowana z procesorem
Wyposażenie multimedialne	Karta dźwiękowa min. Dwukanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo.
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. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25” typu slim. 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. 180W 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) oraz posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: 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 umieszonym na obudowie oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Urządzenie powinno posiadać zabezpieczony (np. 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 oznaczenie producenta (np. logo producenta komputera) 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).
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: ● narrator odczytujący zawartość ekranu, ● lupa powiększająca 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. 23. 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.).
Dodatkowe oprogramowanie	Oprogramowanie producenta komputera z nieograniczoną czasowo licencją 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, - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania) - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. W ofercie należy podać nazwę oprogramowania
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	Deklaracja zgodności CE Urządzenia muszą być wyprodukowane, zgodnie z normą ISO 9001 lub normą równoważną oraz ISO 50001 lub normą równoważną.
Wymagania dodatkowe	Wbudowane porty: 1 x HDMI 1.4 1 x DisplayPort 1.4 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: - Panel przedni: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 - Panel tylny: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu 1 x RJ – 45 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. 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 oznaczeniem (np. 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 Nagrywarka DVD +/-RW o prędkości min. 8x
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 (lub normą równoważną) oraz wykazana zgodnie z normą ISO 9296 (lub normą równoważną) w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 26 dB
Wsparcie techniczne producenta	Dedykowany portal techniczny, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej (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	3-letnia gwarancja na miejscu u klienta. Serwis w języku polskim a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego. Wymagane wsparcie (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. Czas reakcji serwisu – do końca następnego dnia roboczego, Serwis realizowany w systemie door to door W przypadku awarii dysk twardy zostaje u Zamawiającego.
Monitor	Typ ekranu: Ekran ciekłokrystaliczny z aktywną matrycą min. 23,8” (16:9) Technologia wykonania matrycy: IPS Rozmiar plamki: maksymalnie 0,275mm Jasność: min. 250 cd/m2 Kontrast Typowy: 1000:1 Czas reakcji matrycy: max. 8 ms Rozdzielczość maksymalna: 1920 x 1080 przy 60Hz Powłoka powierzchni ekranu: antyodblaskowa utwardzona Podświetlenie: system podświetlenia LED

	Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie. Złącza: min. 1x D-Sub, 1x Display Port 1.2 Gwarancja: 3 lata, możliwość zgłaszania awarii przez linię telefoniczną i stronę internetową Czas reakcji serwisu - do końca następnego dnia roboczego Serwis w języku polskim a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego
Ilość	15 kpl.

Mobilna stacja robocza z oprogramowaniem

Nazwa	Minimalne wymagania dla sprzętu
Typ	Mobilna stacja robocza z oprogramowaniem
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Wbudowany wyświetlacz	Matryca o przekątnej 14.0", rozdzielczość 1920 x 1080. Jasność matrycy 250 cd/m2, kontrast 500:1, matryca bez dotyku Anti-glare
Procesor	Procesor osiągający w teście PassMark Performance Test, co najmniej 12 800 punktów w kategorii Average CPU Mark wg stanu na dzień 4 października 2022 r. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php
Pamięć RAM	16 GB, DDR4, 3200 MHz, dual channel
Pamięć masowa	512 GB NVMe
Karta graficzna	Wynik karty graficznej w teście PassMark Performance Test co najmniej 2760 punktów w kategorii Average G3D Rating wg stanu na dzień 4 października 2022 r. Wynik dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php
Klawiatura	Klawiatura w układzie QWERTY, z wbudowanym w klawiaturze podświetleniem (układ US - QWERTY), 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 min. 2W. Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy. Kamera internetowa z diodą informującą o aktywności, 2 Mpix, trwale zainstalowana w obudowie matrycy wyposażona w mechaniczną przysłonę. 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Wi-Fi 6E (802.11ax) + Bluetooth 5.2
Bateria i zasilanie	Min. 4-cell o pojemności min. 58WHr. Umożliwiająca jej szybkie naładowanie do poziomu 35% w czasie 20 minut i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy min. 65W typ C
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane. Komputer spełniający normy MIL-STD-810H lub równoważne.
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. Niezmazywalne (nieedytowalne) pole asset tag. Funkcje logowania się do BIOS na podstawie hasła użytkownika/systemowego, administratora (hasła niezależne), możliwość ustawienia haseł administratora oraz użytkownika/systemowego składających się z małych liter, dużych liter, cyfr, znaków specjalnych, hasła dla dysku. BIOS zawierający informację o stanie naładowania baterii (stanu użycia), mocy podpiętego zasilacza, ponadto możliwość 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 ISO 9001 lub równoważny dla producenta sprzętu Certyfikat ISO 14001 lub równoważny dla producenta sprzętu Certyfikat ISO 50001 lub równoważny dla producenta sprzętu Deklaracja zgodności CE
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub normą równoważną oraz wykazana zgodnie z normą ISO 9296 lub normą równoważną w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 22dB
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 oraz bez podłączania dodatkowych urządzeń wewnętrznych oraz zewnętrznych, dostępu do sieci i internetu oraz bez konieczności pobierania i instalowania np. w ukrytej pamięci flash BIOS.
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, współpracujący z BIOS z zapisem zdarzeń, informujący administratora o otwarciu komputera. Czytnik linii papilarnych Czytnik SmartCard
Zarządzanie zdalne	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: ➢ monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; ➢ zdalną konfigurację ustawień BIOS, ➢ zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; ➢ zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie; ➢ zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej. ➢ technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/) ➢ nawiązywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS. ➢ wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego ➢ sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji ➢ w pełni aktywna konsola zarządzania wyświetlająca informacje i zachowująca pełną funkcjonalność nawet podczas restartów komputera zarządzanego.
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: ● narrator odczytujący zawartość ekranu, ● lupa powiększająca 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 dodatkowe	Dołączone do oferowanego komputera oprogramowanie 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, 1 x USB 3.2 gen 1 dosilone, 2 x Thunderbolt 4, gniazdo linki zabezpieczającej.
Wsparcie techniczne	Dedykowany portal techniczny, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej (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 gwarancyjne	Serwis w języku polskim a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego. Wymagane wsparcie (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. Minimalny czas trwania wsparcia technicznego wynosi 3 lata Sposób realizacji usług wsparcia technicznego: - Telefoniczne zgłaszanie usterek w trybie 24h / dobę, 7 dni w tygodniu (w języku polskim w dni robocze w godz. 8-17). - Dostęp do bezpłatnego portalu technicznego, który umożliwi zamawianie części zamiennych lub wizyt serwisu, mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy lub serwis przybędzie na miejsce na następny dzień roboczy od momentu przyjęcia zgłoszenia Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń. Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia również dla urządzeń z nieaktywnym wsparciem technicznym. Dostawca zapewni oprogramowanie do automatycznej diagnostyki, zdalnego zgłaszania awarii do serwisu i automatycznego zakładania zgłoszeń serwisowych.
Ilość	1 kpl.

Urządzenie wielofunkcyjne A0

Nazwa	Minimalne wymagania dla sprzętu
Typ	Skaner A0 z funkcją druku

Skaner	Zintegrowany z konstrukcją drukarki (w jednej obudowie)
Technologia skanera	LED
Optyczna rozdzielczość skanowania	Nie mniej niż 600 x 600 dpi
Maksymalna szerokość skanowania	Min. 914 mm (36”)
Maksymalna długość skanowania	Min. 2,5 m
Opcje skanowania	Skanowanie do Email, Skanowanie do FTP, Skanowanie do folderu sieciowego, Skanowanie do USB
Formaty skanowania	JPEG, TIFF, multi-TIFF, PDF, secure PDF, PDF/A, PDF multi
Technologia druku	Atramentowa pigmentowa (wszystkie kolory), odporna na wilgoć
format	Min. A0, 36”
Ilość wkładów z atramentem	Min. 4 (CMYK) – osobno każdy kolor
Wielkość kropli	Min. 4 pl na kolor
Rozdzielczość druku mono	2400 x 1200 dpi
Rozdzielczość druku w kolorze	2400 x 1200 dpi
Podajnik papieru w arkuszach	Min. 50 kartek A4/A3
Taca odbiorcza	Tak
Podstawa z koszem	Tak
Szerokość rolki	Do: 36 cali
Średnica rolki	Min. 110 mm
Obsługiwane rodzaje nośników	Papier zwykły, papiery powlekane i niepowlekane, nabłyszczane, folie, płótna, papier plakatowy;
Obsługiwane formaty nośników	A1, A3, A4, A2, 24", 17", 36", A2+, A3+, A6, B1, B2, B3, B4, B5, rolka 17" (43.2 cm), rolka 24" (61.0 cm), rolka 36" (91.4 cm), A0
Zainstalowana pamięć	Min. 1 GB RAM
Interfejsy	Hi-Speed USB – kompatybilny z USB 2.0, Ethernet Interface (1000 Base-T/ 100-Base TX/ 10-Base-T), Wireless LAN IEEE 802.11a/b/g/n/ac
Druk z pamięci USB	TAK
Odcinanie nośnika	automatyczne
Zużycie energii	Max 24 W
Waga urządzenia wraz z podstawą	Max. 54 kg
Wymagania systemowe	Mac OS X 10.6.8 or later, Windows 10, Windows 7 (32/64 bit), Windows 8.1 (32/64 bit), Windows Vista (32/64 bit), Windows XP
Opcje bezpieczeństwa	SNMP, IPSec, POPS, FTP, WPA3, IEEE802, SSL/TLS
Gwarancja	Gwarancja 24 miesiące z naprawą na miejscu w siedzibie odbiorcy urządzenia, bez dodatkowych kosztów wynikających z przeglądów gwarancyjnych. Gwarancja obejmująca również głowicę drukującą.
Ilość	1 kpl.

Oprogramowanie do monitorowania sieci i pracowników

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Oprogramowanie do monitorowania sieci i pracowników
Wymagania minimalne	Rozszerzenie posiadanej przez Zamawiającego licencji na oprogramowanie Axence nVision o Smart Time z wyrównaniem umowy serwisowej lub zaoferowanie rozwiązania równoważnego Obecna umowa zawarta jest do dnia 18 lutego 2023 r. Ilość licencji- 110. Zamawiający wymaga dostarczenia licencji na okres 36 miesięcy.
Ilość	1 kpl. – 110 licencji

Oprogramowanie do backupu stacji roboczych

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do backupu i archiwizacji komputerów w sieciach LAN
Wymagania funkcjonalne	• Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich • Program serwerowy kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, Linux, BSD, Mac OS X, QNAP, Synology • Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, Linux, BSD, Mac OS X, QNAP, Synology • Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików) • Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS) • Automatyczny backup przy wyłączaniu komputera • Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ? • Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows) • Backup baz danych i plików poczty w trybie online i offline • Kopie rotacyjne (wersjonowanie) • Zapis archiwów w otwartym formacie (ZIP 64-bit) • Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore) • Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej • Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych • Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO • Kompresja po stronie stacji roboczej • Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP, • Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows) • Centralne sterowanie całym Systemem z jednego miejsca • Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników • Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN • Wysyłanie Alertów administracyjnych na e-mail • Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych • Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki • Automatyczna aktualizacja oprogramowania na komputerach zdalnych
Licencja	Licencja dla: 120 stanowisk klienckich Bezterminowa licencja - licencja nie może być ograniczona czasowo Licencja powinna posiadać dodatkowe wsparcie techniczne na okres minimum 36 miesięcy.
Wymagania dodatkowe	Interfejs, instrukcja i pomoc techniczna w języku polskim
Ilość	1 kpl.

Urządzenia do backupu - typ I

Nazwa	Minimalne wymagania dla sprzętu

Typ	Urządzenia do tworzenia backupu
Specyfikacja sprzętowa	Procesor 64 bit Procesor liczba rdzeni: nie mniej niż 4 Pamięć RAM: nie mniej niż 8GB Pamieć 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 12 Obsugiwane dyski twarde 3.5" oraz 2.5” SATA, 2.5" SATA SSD Pojemność dysków twardych możliwych do stosowania: min. do 18 TB Możliwość podłączenia modułu rozszerzającego: Tak, co najmniej dwóch Porty LAN GbE: minimum 2x 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: Tak, minimum 1 Przyciski min.: Reset, Zasilanie Typ obudowy: RACK, 2U Dopuszczalna temperatura pracy: od 0 do 40˚C Zasilanie Zasilacz redundatny 2 x 250 W, 100-240 V
Specyfikacja oprogramowania	Agregacja łączy: Tak Obsługiwane systemy plików: - Dyski wewnętrzne: EXT4 - Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ Możliwość podłączenia karty WLAN na USB: Tak Szyfrowanie wolumenów: Tak, min AES 256 Szyfrowanie dysków zewnętrznych: Tak 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 - Obsługa replikacji migawek - Wbudowana obsługa iSCSI - Multi-LUNs na Target - Obsługa LUN Mapping & Masking - Obsługa SPC-3 Persistent Reservation - Obsługa MPIO & MC/S, - Migawka / kopia zapasowa iSCSI LUN 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 podłączenia do 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: - Minimum: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box Darmowe aplikacje na urządzenia mobilne: - Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki - 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 - Całkowity rejestr systemowy (poziom pliku) - Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line - Aktualizacja oprogramowania - Możliwość ręcznej aktualizacji 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 - Połączenie HTTPS - FTP z SSL/TLS (Explicit) - Szyfrowanie AES 256-bit - Zdalna replikacja - Import certyfikatu SSL - Powiadomienia o zdarzeniach za pośrednictwem Email i SMS Możliwość instalacji dodatkowego oprogramowania i możliwość instalacji z paczek
Wymagania dodatkowe	W ramach dostawy Zamawiający wymaga dodatkowo dostarczenia: a) Zainstalowane dyski minimum: - 12 x dysków min. 6TB 3,5" 256MB SATAIII/7200rpm b) Karta komunikacyjna umożliwiająca zasilaczowi UPS komunikację z innymi rodzajami urządzeń. Karta musi umożliwiać m.in. podłączenie min. 3 czujników warunków środowiskowych w celu kontroli wilgotności, temperatury, sygnałów z czujników dymu i innych informacji dotyczących bezpieczeństwa. c) zasilacz awaryjny o parametrach minimalnych: - Moc pozorna: min. 1000VA - Moc rzeczywista: min. 1000W - Technologia: on-line (VFI), podwójna konwersja - Sprawność max (dla VFI): > 87 % - Typ obudowy: rack/tower - Ilość wydzielanego ciepła dla nominalnych warunków pracy: < 510 BTU / h - Napięcie wejściowe: 110 ÷ 300 V AC ± 5% - Częstotliwość napięcia wejściowego: 50 / 60 Hz

	- Zakres napięcia wyjściowego: 208 V AC / 220 V AC / 230 V AC / 240 V AC ± 1 % - Wartość napięcia wyjściowego ustawiana z panelu LCD: tak - Kształt napięcia wyjściowego: sinusoidalny - Czas przełączania sieć – UPS: 0ms - Współczynnik odkształceń prądu wejściowego THDi: < 10% - Napięcie wyjściowe: ~230V - Częstotliwość napięcia wyjściowego 50Hz/60Hz ± 0,5Hz - Kształt napięcia wyjściowego na pracy bateryjnej: sinusoidalny - Zabezpieczenie przeciążeniowe: elektroniczne - Akumulatory wewnętrzne w UPS: minimum 12V 9Ah; szczelne, bezobsługowe - Czas podtrzymania dla obciążenia 85W - przy zastosowaniu wyłącznie wewnętrznych baterii: minimum 115 minut - Czas ładowania baterii wew w UPS i w modułach bateryjnych (niezależnie od ilości podłączonych modułów) - po 80% wyładowaniu baterii: do 3h - Ilość i typ gniazd wyjściowych: minimum 6x IEC 320 C13 (10 A) - Sygnalizacja: wyświetlacz LCD - Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych - Wymagana możliwość podłączenia do 10 zewnętrznych modułów bateryjnych - Test baterii: wymagana możliwość uruchomienia testu baterii przyciskiem na obudowie zasilacza - Uszkodzony akumulator: wymagany komunikat wyświetlany na wyświetlaczu LCD - Interfejs komunikacyjny: RS232, USB HID, SNMP - Wsporniki do montażu w szafie RACK: wymagane - Remote ON/OFF – możliwość zdalnego załączenia/wyłączenia zasilacza: wymagane - Możliwość pracy w trybie konwertera częstotliwości: wymagane - Zabezpieczenia: minimum przeciwzwarciowe, przeciwprzepięciowe, przeciążeniowe, termiczne - Gwarancja: minimum 24 miesiące na elektronikę i 24 miesiące na akumulatory; d) Szafa rack: 19”, wysokość min. 10U maks 12U, szerokość i głębokość: 600 mm x 600 mm
Gwarancja	Minimum 36 miesięcy
Ilość	2 kpl.

Urządzenia do backupu - typ II

Nazwa	Minimalne wymagania dla sprzętu
Typ	
Specyfikacja sprzętowa	Procesor minimum 64 bit x86 Procesor liczba rdzeni: nie mniej niż 4 Pamięć RAM: nie mniej niż 8GB Pamieć RAM liczba slotów: minimum 2 sloty Pamięć RAM - możliwość rozszerzenia: nie mniej niż do 64GB Pamięć Flash: nie mniej niż 5 GB Liczba zatok na dyski: minimum 4 zatoki 3,5" Obsugiwane dyski 3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD Wbudowane w urządzenie interfejsy na dyski M2: min. 2 x M2 PCIe Gen3x1 Możliwość stosowania dysków twardych o pojemności: min. do 18TB Możliwość podłączenia modułu rozszerzającego: Tak, co najmniej 2 Porty LAN 2,5 GbE” minimum 2 RJ-45 Diody LED: minimum Status, LAN, HDD Porty USB 3.2 Gen2: minimum 3 Port PCiE: Tak, minimum 2 Gen3x4 Przyciski min.: Reset, Zasilanie Typ obudowy: Tower Dopuszczalna temperatura pracy: od 0 do 40°C Zasilanie Max. 250 W
Specyfikacja oprogramowania	Obsługa dwóch systemów operacyjnych: - Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS

Wymagania dla systemu operacyjnego opartego o system plików EXT4	Agregacja łączy Obsługiwane systemy plików: - Dyski wewnętrzne: EXT4 - Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT Możliwość podłączenia karty WLAN na USB: Tak Szyfrowanie udziałów: Tak, min AES 256 Szyfrowanie dysków zewnętrznych: Tak Zarządzanie dyskami: - Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, - Obsługa Hot Spare per grupa RAID oraz global hot spare - Rozszerzanie pojemności Online RAID - Migracja poziomów Online RAID - HDD S.M.A.R.T. - Skanowanie uszkodzonych bloków - Przywracanie macierzy RAID - Obsługa map bitowych - Pula pamięci masowej - Obsługa migawek - Obsługa replikacji migawek Wbudowana obsługa iSCSI: - Multi-LUNs na Target - Obsługa LUN Mapping & Masking - Obsługa SPC-3 Persistent Reservation - Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN 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 plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, Współpraca z zewnętrznymi dostawcami usług chmury co najmniejGoogle Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box Darmowe aplikacje na urządzenia mobilne: - Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer - Dostępne na co najmniej 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 - Całkowity rejestr systemowy (poziom pliku) - Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line - Aktualizacja oprogramowania automatyczna - Możliwość aktualizacji oprogramowania ręcznie - Ustawienia systemu: Kopia, Przywracanie, Resetowanie" Wirtualizacja: - Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 - Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. Konteneryzacja: - Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker Zabezpieczenia: - Filtracja IP - Ochrona dostępu do sieci z automatycznym blokowaniem - 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 i możliwość instalacji z paczek
Wymagania dodatkowe	Zainstalowane dyski: minimum 4x dyski min. 2TB 3,5cal SATA 6Gb/s 128MB Cache
Gwarancja	Minimum 36 miesięcy
Ilość	1 kpl.

Urządzenia do backupu - typ III

Nazwa	Minimalne wymagania dla sprzętu
Parametry techniczne	a) Obudowa typu RACK 19” o wysokości 1U b) Minimalna liczba interfejsów sieciowych urządzenia to 1 interfejs sieciowy 1 Gigabit. c) Przestrzeń dyskowa o pojemności min. 6TB d) Redundantna macierz dysków typu SW RAID 10 e) Wymienne dyski f) Redundantne zasilanie z możliwością wymiany w trakcie pracy urządzenia. Oferowane rozwiązanie musi posiadać deklarację zgodności CE
Administracja	a) Rozwiązanie ma być konfigurowane za pomocą graficznego interfejsu dostępnego przez przeglądarkę internetową. b) Rozwiązanie może być zarządzane przez dowolną liczbę administratorów, którzy posiadają rozłączne lub nakładające się uprawnienia. c) Rozwiązanie powinno posiadać mechanizm informowania administratorów o wystąpieniu błędów za pośrednictwem automatycznie generowanych wiadomości poczty elektronicznej. Rozwiązanie backupowe powinno posiadać opcję informowania w formie wiadomości e-mail o statusie wykonania zadań backupowych na więcej niż jeden adres e-mail.
Backup danych	a) Rozwiązanie musi zapewnić funkcjonalność scentralizowanego systemu wykonywania kopii zapasowych w heterogenicznym środowisku (różne systemy operacyjne) z wykorzystaniem następujących protokołów: SMB, CIFS, b) Rozwiązanie musi wspierać archiwizację danych z systemów Mac OS X. c) Rozwiązanie ma wspierać archiwizację poczty na poziomie pojedynczej wiadomości z systemów Microsoft Exchange.

	d) Producent zobowiązany jest dostarczyć dedykowanego Agenta do systemów Windows, za pomocą, którego możliwe jest archiwizowanie danych z Microsoft Exchange, Microsoft SQL, Microsoft Hyper-V, Microsoft Active Directory oraz rejestru systemowego, stanu systemu operacyjnego (ang. System State) i plików przechowywanych na dyskach systemu Microsoft Windows. Agent backupu dostarczany jest dla systemów operacyjnych aktualnie wspieranych przez firmę Microsoft. e) Agent dla systemów z rodziny Microsoft Windows ma wspierać mechanizm deduplikacji danych. f) Agent nie wymaga dodatkowej licencji i może być zainstalowany na dowolnej liczbie komputerów. g) Rozwiązanie ma wspierać archiwizację otwartych i edytowanych plików. h) Rozwiązanie ma posiadać funkcję automatycznego backupu otwartego i edytowanego pliku. i) Rozwiązanie ma umożliwiać wykonywanie backapu w oparciu o harmonogram utworzony przez administratora. j) Rozwiązanie musi umożliwiać definiowanie różnych strategii wykonywania backapu dla poszczególnych obiektów podlegających backupowi. k) Rozwiązanie musi mieć możliwość wykonywania backupu na lokalnie dostarczonym urządzeniu l) Rozwiązanie backupowe powinno umożliwiać zarządzanie wieloma urządzeniami tego samego typu przy użyciu jednego interfejsu graficznego. m) Rozwiązanie musi umożliwiać replikacji danych zapisanych na urządzeniu na zewnętrzne nośniki typu taśmy, VTL, NAS n) Rozwiązanie musi umożliwiać wykonywanie backup PTV systemów z rodziny Windows na VMware
Odtwarzanie danych	a) Odtwarzanie danych może odbywać się przy użyciu następujących mechanizmów: • dedykowanego klienta odtwarzania dla systemów Windows, • interfejsu WWW, b) Dane mogą być odtwarzane przez administratorów urządzenia lub użytkowników końcowych w zależności od uprawnień. c) Możliwość uruchomienia backupu wirtualnego na urządzeniu producenta dla VMWare • Bare Metal Live CD dla takich systemów jak: Windows Vista / 7 / 8 / 10 / 2008 Server / 2008 Server R2 / 2012 Server / 2012 Server R2 / 2016 Server
Raportowanie	a) Rozwiązanie backupowe powinno udostępniać raporty pozwalające na analizę kluczowych elementów, takich jak: b) archiwizowania i odtwarzania danych, c) wykorzystania dostępnych zasobów dyskowych i systemowych d) Rozwiązanie backupowe powinno udostępniać raporty pozwalające na analizę aktywności administratorów i użytkowników. • Rozwiązanie backupowe powinno udostępniać pełną historię modyfikacji zarchiwizowanych plików.
Gwarancja i wsparcie techniczne	Minimum 36 miesięcy gwarancji obejmującą wsparcie techniczne oraz aktualizacje modułów oprogramowania urządzenia. W ramach gwarancji wymagany jest także dostęp do najnowszej wersji oprogramowania i aktualnej ochronę. Wszystkie aktualizacje muszą być automatyczne i nie mogą wymagać ingerencji klienta końcowego; - w przypadku awarii urządzenia, wysyłka nowego, zastępczego urządzenia odbędzie się najpóźniej następnego dnia roboczego; - dostęp do wirtualnego urządzenia backupowe na potrzeby przechowywania danych (wsparcie głównego serwera danych).
Ilość	1 kpl.

Wymagania dodatkowe dla części I

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 Zamawiającego.

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 Zamawiającego.

Część II Przedmiotu zamówienia

Certyfikowane szkolenie dla administratora z dostarczonych rozwiązań oraz z zakresu cyberbezpieczeństwa

Nazwa	Minimalne wymagania dla szkoleń
Szkolenie typ I	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego urządzenia klasy UTM Program szkolenia – zakres minimalny: 1. Architektura FortiManagera Główne funkcjonalności urządzenia Przegląd interfejsu administratora Koncepcja ADOM Porównanie FortiManager - FortiAnalyzer 2. Konfiguracja opcji systemowych System dashboard Backup i przywracanie po awarii Aktualizacja firmware Role administratorów Uruchamianie funkcjonalności FortiAnalyzera Tryb workspace/workflow 3. Zarządzanie urządzeniami - Device Manager Metody dodawania urządzeń Provisioning templates Status konfiguracji Configuration Revision 4. Zarządzanie politykami i obiektami – Policy & Objects Zarządzanie politykami na poziomie ADOM Dynamiczne mapowanie interfejsów i obiektów ADOM Revision – tworzenie i odzyskiwanie 5. Zaawansowana konfiguracja i rozwiązywanie problemów. Interfejs „command line” Zarządzanie licencjami Aktualizacja zarządzanych urządzeń Skrypty, obiekty CLI-Only Offline mode Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Ilość: Szkolenie dla 1 administratora
Szkolenie typ II	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Omówienie administracji Windows Server Wprowadzenie do Windows Server 2019 Omówienie systemu Windows Server Core Omówienie zasad i narzędzi administracyjnych systemu Windows Server 2.Usługi tożsamości w systemie Windows Server Przegląd usług AD DS. Wdrażanie kontrolerów domeny systemu Windows Server Omówienie usługi Azure AD Wdrażanie Group Policy Omówienie Usług certyfikatów w usłudze Active Directory 3.Usługi infrastruktury sieciowej w systemie Windows Server

	Wdrażanie i zarządzanie DHCP Wdrażanie i zarządzanie usługą DNS Wdrażanie i zarządzanie IPAM Usługi dostępu zdalnego w systemie Windows Server 4.Serwery plików i zarządzanie pamięcią masową w systemie Windows Server Woluminy i systemy plików w systemie Windows Server Wdrażanie udostępniania w systemie Windows Server Wdrażanie miejsc do magazynowania w systemie Windows Server Wdrażanie deduplikacji danych Wdrażanie iSCSI Wdrażanie rozproszonego systemu plików 5.Wirtualizacja i kontenery Hyper-V w systemie Windows Server Hyper-V w systemie Windows Server Konfigurowanie maszyn wirtualnych Zabezpieczanie wirtualizacji w systemie Windows Server Kontenery w systemie Windows Server Omówienie Kubernetes 6.Wysoka dostępność w systemie Windows Server Wysoka dostępność w systemie Windows Server Planowanie wdrożenia klastra pracy awaryjnej Tworzenie i konfigurowanie klastra pracy awaryjnej Przegląd klastrów typu stretch Wysoka dostępność i rozwiązania do odzyskiwania po awarii maszyn wirtualnych 7.Odzyskiwanie po awarii w systemie Windows Server Replika Hyper-V Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server 8.Bezpieczeństwo systemu Windows Server Poświadczenia i ochrona dostępu uprzywilejowanego Hardening Windows Server JEA w systemie Windows Server Zabezpieczanie i analizowanie ruchu SMB Zarządzanie aktualizacjami systemu Windows Server 9.RDS w systemie Windows Server Przegląd usług RDS Konfigurowanie wdrożenia pulpitu opartego na sesji Przegląd osobistych i połączonych wirtualnych pulpitów 10.Dostęp zdalny i usługi internetowe w systemie Windows Server Wdrażanie VPN Wdrażanie Always On VPN Wdrażanie usługi NPS Wdrażanie serwera internetowego w systemie Windows Server 11.Monitorowanie serwera i wydajności w systemie Windows Server Omówienie narzędzi do monitorowania systemu Windows Server Korzystanie z monitora wydajności Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów 12.Aktualizacja i migracja w systemie Windows Server Migracja usług AD DS. Usługa migracji pamięci masowej Narzędzia migracji systemu Windows Server Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Ilość: Szkolenie dla 1 administratora
Szkolnie typ III	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Wprowadzenie Informacje o szkoleniu Agenda szkolenia Środowisko laboratoryjne

	2.Wprowadzenie do usługi AD DS w Windows Server 2022 Active Directory – omówienie Co nowego w Active Directory? Budowa logiczna usługi AD DS Budowa fizyczna usługi AD DS Działanie usługi AD DS 3.Instalacja usługi AD DS w Windows Server 2022 Wdrażanie usług AD DS Wdrażanie i klonowanie wirtualnych kontrolerów domeny Wdrażanie kontrolerów domeny w systemie Windows Azure 4.Administrowanie AD DS Graficzne konsole administracyjne Narzędzia linii poleceń Zarządzanie obiektami za pomocą PowerShell Typowe czynności administracyjne 5.Replikacja bazy AD Omówienie replikacji usług AD DS Konfigurowanie lokacji AD DS. 6.Zabezpieczanie AD DS Bezpieczeństwo kontrolerów domeny Wzorce operacji 7.Monitorowanie i odzyskiwanie usług AD DS Monitorowanie AD DS Zarządzanie bazą danych AD DS Opcje tworzenia kopii zapasowych i odzyskiwania AD DS 8.Wdrażanie polityk GPO Wprowadzenie do zasad grupy Wdrażanie i administrowanie obiektami GPO Rozwiązywanie problemów z zastosowaniem obiektów zasad grupy 9.Konfiguracja środowiska pracy użytkownika za pomocą zasad grupy Szablony administracyjne Konfigurowanie przekierowania folderu i skryptów Instalacja oprogramowania Konfigurowanie preferencji zasad grupy 10.Konfiguracja dynamicznej kontroli dostępu DAC (Dynamic Access Control) Wdrażanie komponentów DAC Konfiguracja DAC Wdrażanie pomocy odmowy dostępu 11.Wdrażanie i zarządzanie usługami AD CS Wdrażanie roli AD CS Administrowanie urzędami certyfikacji Zarządzanie szablonami certyfikatów Korzystanie z certyfikatów w środowisku biznesowym 12.Wdrażanie i zarządzanie AD RMS Omówienie AD RMS Wdrażanie i zarządzanie infrastrukturą AD RMS Konfigurowanie ochrony treści AD RMS 13.Wdrażanie i zarządzanie usługami AD FS Omówienie usług AD FS Wdrażanie usług AD FS 14.Wdrażanie Windows Azure Active Directory (opcjonalnie) Omówienie usługi Windows Azure AD Zarządzanie kontami Windows Azure AD Synchronizacja kont AD DS z Azure AD Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Ilość: Szkolenie dla 1 administratora
Szkolenie typ IV	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych

	Program szkolenia – zakres minimalny: 1.Przygotowanie infrastruktury Active Directory do zarządzania zasadami grupy Potrzeby organizacji w zakresie scentralizowanego zarządzania ustawieniami dla komputera i użytkownika Potrzeby organizacji w zakresie zapewnienia założonego poziomu bezpieczeństwa Infrastruktura Active Directory Komponenty infrastruktury sieciowej Projektowanie infrastruktury jednostek organizacyjnych pod kątem efektywnego stosowania zasad grupy 2.Wprowadzenie do Windows PowerShell Wprowadzenie do Windows PowerShell Polecenia modułu GroupPolicy. Dodatkowe moduły do zarządzania GPO z PowerShell Gallery Skrypty logowania Zarządzanie zdalne 3.Wprowadzenie do zarządzania konfiguracją komputera i użytkownika Zarządzania konfiguracją Zarządzanie konfiguracją za pomocą zasad grupy Nowe funkcje zasad grupy wprowadzone w kolejnych wersjach Windows Server Wykorzystanie Windows PowerShell w procesie zarządzania konfiguracją 4.Narzędzia do zarządzania zasadami grupy Zasady lokalne i domenowe Konsola zarządzania zasadami grupy (GPMC) Proces odświeżania GPO Konfiguracja zasad grupy do zdalnego zarządzania za pomocą Server Manager 5.Wprowadzenie do zarządzania i przetwarzania zasad grupy Uprawnienia do zarządzania obiektami zasad grupy Komponenty zasad grupy w Active Directory Proces przetwarzania zasad grupy Modyfikacja procesu przetwarzania zasad grupy 6.Zapewnienie założonego poziomu zabezpieczeń za pomocą zasad grupy Komponenty architektury zabezpieczeń dla systemu Windows Bezpieczeństwo konta użytkownika Polityka lokalna Zaawansowana inspekcja Hardening środowiska Windows Zarządzanie certyfikatami za pomocą zasad grupy Analiza dziennika zabezpieczeń 7.Zapewnienie bezpieczeństwa aplikacji za pomocą zasad grupy Zarządzanie ustawieniami UAC Ochrona przed złośliwym oprogramowaniem Wykorzystanie AppLocker do ograniczeń aplikacji 8.Konfiguracja środowiska stacji roboczych Typy skryptów i kontrola ich wykonywania Ustawienia pulpitu, Menu Start oraz paska zadań Ustawienia panelu sterowania Komponenty Windows Zarządzanie drukarkami Ustawienia sieci 9.Wirtualizacja stanu użytkownika Konfiguracja przekierowania folderów Zarządzanie plikami Offline Wdrożenie User Experience Virtualization 10.Zarządzanie instalacją oprogramowania za pomocą zasad grupy Dystrybucja aplikacji za pomocą paczek MSI Punkty dystrybucyjne aplikacji Zarządzanie pakietami 11.Szablony administracyjne Wprowadzenie do szablonów administracyjnych Zarządzanie szablonami ADMX Przygotowanie i zarządzanie Central Store

	Wdrażanie i zarządzanie oprogramowaniem Microsoft oraz firm trzecich za pomocą szablonów administracyjnych 12.Preferencje zasad grupy Wprowadzenie do preferencji zasad grupy Porównanie preferencji i polityk grupowych Opcje konfiguracyjne preferencji 13.Rozwiązywanie problemów i kopia zapasowa Narzędzia do rozwiązywania problemów Wynikowe zasady grupy (RSOP) Podgląd zdarzeń Kopia zapasowa, przywracanie, importowanie i kopiowanie obiektów zasad grupy Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Ilość: Szkolenie dla 1 administratora
Szkolenie typ V	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Podstawowe pojęcia związane z platformą Azure Wprowadzenie do podstaw platformy Azure Podstawowe pojęcia dotyczące platformy Azure Podstawowe składniki architektoniczne platformy Azure 2.Podstawowe usługi Azure Usługi bazy danych i analizy platformy Azure Usługi obliczeniowe platformy Azure Usługi Azure Storage Usługi sieciowe platformy Azure 3.Opis podstawowych rozwiązań i narzędzi do zarządzania na platformie Azure Wybieranie usługi AI do swoich potrzeb Wybieranie narzędzia, aby pomóc organizacjom w tworzeniu lepszych rozwiązań Wybieranie usługi monitorowania pod kątem widoczności, wglądu i ograniczania przestojów Wybieranie narzędzia do zarządzania i konfigurowania środowiska platformy Azure Wybieranie bezserwerowej technologii Azure dla swojego scenariusza biznesowego 4.Opis ogólnych zabezpieczeń i funkcji bezpieczeństwa sieci Ochrona przed zagrożeniami bezpieczeństwa na platformie Azure Bezpieczna łączność sieciowa na platformie Azure 5.Opis funkcji tożsamości, zarządzania, prywatności i zgodności Zabezpieczenie dostępu do swoich aplikacji, korzystając z usług tożsamości platformy Azure Utworzenie strategii zarządzania chmurą na platformie Azure Sprawdzenie standardów prywatności, zgodności i ochrony danych na platformie Azure 6.Opis zarządzania kosztami platformy Azure i umów dotyczących poziomu usług Planuj i zarządzaj kosztami platformy Azure Wybierz odpowiednie usługi platformy Azure, analizując umowy SLA i cykl życia usługi Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - Uczestnik po zakończeniu szkolenia musi mieć możliwość przystąpienia do certyfikowanego egzaminu: w autoryzowanym centrum egzaminacyjnym, online będąc monitorowanym przez zewnętrznego egzaminatora Ilość: Szkolenie dla 1 administratora
Szkolenie typ VI	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Tożsamość

	Azure Active Directory Użytkownicy i grupy 2.Zarządzanie i zgodność Subskrypcje i konta Zasady platformy Azure Kontrola dostępu oparta na rolach (RBAC) 3.Administracja Azure Azure Resource Manager Azure Portal i Cloud Shell Azure PowerShell i interfejs wiersza polecenia Szablony ARM 4.Sieć wirtualna Sieci wirtualne Adresowanie IP Grupy bezpieczeństwa sieci Zapora Azure Azure DNS 5.Łączność międzylokacyjna Peering sieci wirtualnej Połączenia bramy VPN ExpressRoute i wirtualna sieć WAN 6.Zarządzanie ruchem w sieci Network Routing i EndpointsAzure Load Balancer Azure Application Gateway Traffic Manager 7.Azure Storage Konta magazynu Magazyn obiektów blob Bezpieczeństwo przechowywania Pliki platformy Azure i synchronizacja plików Zarządzanie pamięcią masową 8.Azure Virtual Machines Planowanie maszyny wirtualnej Tworzenie maszyn wirtualnych Dostępność maszyny wirtualnej Rozszerzenia maszyny wirtualnej 9.Obliczenia bezserwerowe Plany Azure App Service Usługa aplikacji Azure Usługi kontenerowe Usługa Azure Kubernetes 10.Ochrona danych Kopie zapasowe plików i folderów Kopie zapasowe maszyn wirtualnych 11.Monitorowanie Azure Monitor Azure alerts Log Analytics Network Watcher Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - Uczestnik po zakończeniu szkolenia musi mieć możliwość przystąpienia do certyfikowanego egzaminu Ilość: Szkolenie dla 1 administratora
Szkolenie typ VII	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1. Wprowadzenie do SI

	• Sztuczna inteligencja w Azure • Odpowiedzialna SI 2. Uczenie maszynowe • Wprowadzenie do uczenia maszynowego • Uczenie maszynowe w Azure 3. Mechanizmy Computer Vision • Koncepcje Computer Vision • Computer Vision w Azure 4. Procesowanie języka naturalnego • Omówienie mechanizmów procesowania języka naturalnego (NLP) w Azure 5. Konwersacyjna SI • Koncepcje konwersacyjnej sztucznej inteligencji • Konwersacyjna SI w Azure Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Ilość: Szkolenie dla 1 administratora
Szkolenie typ VIII	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Introduction to the AWS Cloud 2.Introduction to the AWS Management Console 3.Security in AWS Cloud Identity and Access Management (IAM) IAM Laboratory 4.Network Amazon Virtual Private Cloud (VPC) VPC Laboratory - build your first VPC VPC inter-connectivity options VPC peering laboratory 5.Compute Amazon Elastic Compute Cloud (EC2), EC2 Laboratory - build your first EC2 instance Auto-scaling and load balancing Laboratory - build and autoscaled application Introduction to AWS Lambda Lambda Laboratory - build backend service with AWS Lambda 6.Object Storage Amazon Simple Storage Service (S3) S3 Laboratory - create your first S3 bucket S3 Features overview S3 Website static hosting laboratory Amazon CloudFront (CDN) CloudFront Laboratory 7.Database options Amazon Relational Database Service (RDS) + Aurora RDS Laboratory Amazon Aurora Laboratory Amazon DynamoDB DynamoDB Laboratory 8.Management Services Amazon CloudWatch and CloudTrail CloudTrail laboratory - analyse CloudTrail logs with Amazon Athena AWS CloudFormation Laboratory - deploy solution using CloudFormation Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby:

	- Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - W ramach szkolenia uczestnik musi mieć 2 dni pracy z trenerem w formie **warsztatów** Ilość: Szkolenie dla 1 administratora
Szkolenie typ IX	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Introduction to the AWS Cloud 2.Overview of AWS platform and services 3.Security in AWS Cloud General aspects of security in the cloud Deep Dive into Identity and Access Management service AWS Account Security Laboratories 4.Network Solutions in AWS Network services in AWS Deep dive into Amazon Virtual Private Cloud (VPC) Network security and traffic control Hybrid Connectivity options Laboratories 5.Operation in AWS Cloud Services for daily operation AWS CloudFormation AWS Beanstalk AWS CloudWatch AWS CloudTrail Laboratories 6.Building database solutions Learn difference SQL and NoSQL database NoSQL databases in Amazon Web Services SQL Databases - Amazon Relational Database Service Cloud native databases Cache layer with ElastiCache Laboratories 7.Tooling and Automation on AWS Ways to use AWS AWS Systems Manager Laboratories 8.Monitoring and Managing Resource Consumption Observability on a single platform Improve operational performance and resource optimization Application monitoring Laboratories 9.Cost management in AWS Manage Billing and Control Costs Improved Planning with Flexible Forecasting and Budgeting Optimize Costs with Resource and Pricing Recommendations Laboratories 10.Overview of the Well-Architected Framework Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - W ramach szkolenia uczestnik musi mieć 2 dni pracy z trenerem w formie technicznych **warsztatów** Ilość: Szkolenie dla 1 administratora

Szkolenie typ X	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Bezpieczeństwo w SQL Server Uwierzytelnianie połączeń do SQL Server Autoryzacja dostępu kont logowania do bazy danych Autoryzacja pomiędzy serwerami Bazy danych Partially Contained 2.Przypisywanie ról serwera i bazy danych Praca z rolami serwera Praca z wbudowanymi rolami bazodanowymi Tworzenie własnych ról bazodanowych 3.Autoryzacja dostępu użytkowników do zasobów Autoryzacja dostępu użytkowników do obiektów Autoryzacja dostępu użytkowników do wykonania kodu Konfiguracja uprawnień na poziomie Schemy 4.Ochrona danych przy użyciu szyfrowania i audytu Opcje audytowania dostępu do danych w SQL Server Implementacja audytu SQL Server Zarządzanie audytem SQL Server Ochrona danych przy użyciu szyfrowania 5.Modele odzyskiwania SQL Server i strategie kopii zapasowych Zrozumienie strategii kopii zapasowych Zasady działania logu transakcji w SQL Server Planowanie strategii wykonywania kopii zapasowych 6.Wykonywanie kopii zapasowych Tworzenie kopii zapasowej baz danych i logów transakcji Zarządzanie kopiami zapasowymi Opcje tworzenia kopii zapasowej 7.Odtwarzanie baz danych SQL Server Omówienie procesu odtwarzania Odtwarzanie baz danych Zaawansowane scenariusze odtwarzania baz danych Odtwarzanie kopii zapasowej do punktu w czasie 8.Automatyzacja zarządzania SQL Server Mechanizmy automatyzacji zarządzania SQL Server Praca z usługą agenta SQL Server Zarządzanie zadaniami agenta SQL Server Zarządzanie zadaniami na wielu serwerach 9.Konfiguracja zabezpieczeń dla SQL Server Agent Omówienie zabezpieczeń SQL Server Agent Konfiguracja poświadczeń Konfiguracja kont proxy 10.Monitorowanie SQL Server przy użyciu alertów i powiadomień Monitorowanie błędów SQL Servera Konfiguracja Database Mail Operatorzy, alerty i powiadomienia Alerty w Azure SQL Database 11.Wstęp do zarządzania SQL Server przy użyciu PowerShell Podstawy pracy z Windows PowerShell Konfigurowanie SQL Server przy użyciu PowerShell Utrzymanie środowiska SQL Server przy użyciu PowerShell Utrzymanie Azure SQL Database przy użyciu PowerShell 12.Śledzenie dostępu do SQL Server z użyciem Extended Events Podstawowe pojęcia związane z Extended Events Praca z Extended Events 13.Monitorowanie SQL Server 2017 Monitorowanie aktywności Zbieranie i zarządzanie danymi wydajności Analiza zebranych danych o wydajności SQL Server utility

	14.Rozwiązywanie problemów z SQL Server Metodologia rozwiązywania problemów w SQL Server Rozwiązywanie problemów związanych z usługą Rozwiązywanie problemów z logowaniem i łącznością 15.Importowanie i eksportowanie danych Transferowanie danych do/z SQL Server Importowanie i eksportowanie danych z tabel Używanie BCP i BULK INSERT do importu danych Wdrażanie i aktualizacja aplikacji data-tier Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Ilość: Szkolenie dla 1 administratora
Szkolenie typ XI	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Budowa sieci IP Elementy sieci komputerowych Topologie sieci Standardy sieciowe – przewodowe Standardy sieciowe – bezprzewodowe Karty sieciowe Okablowanie sieciowe Podział sieci wg. Kryterium Urządzenia sieciowe LAB: Budowa sieci IP 2.Model OSI, protokół TCP/IP Potrzeba standaryzacji łączności Model referencyjny OSI Enkapsulacja i de-enkapsulacja danych Rodzaje komunikacji Pakiet protokołów TCP/IP Warstwa transportowa: TCP i UDP Warstwa aplikacji Warstwa Internetu LAB A: Protokół ARP Komunikacja bezpośrednia Komunikacja poprzez przełącznik Komunikacja przez router LAB B: Jak zmieniają się adresy MAC i IP podczas przesyłania pakietów w sieci 3.Adresacja w sieci IP Omówienie adresacji IPv4, klasy adresów, maska Zasady tworzenia podsieci Korzystanie z maski bezklasowej Przypisywanie adresów IPv4 LAB A: Maska, planowanie podsieci LAB B: Przypisywanie i weryfikacja adresów IP 4.Konfiguracja usługi DHCP Protokół DHCP Dodawanie i autoryzowanie usługi serwera DHCP LAB A: Instalacja serwera DHCP Konfigurowanie zakresu DHCP Konfigurowanie zastrzeżenia DHCP LAB B: Wstępna konfiguracja serwera DHCP Konfigurowanie opcji DHCP Konfigurowanie agenta przekazywania LAB C: Dodatkowa konfiguracja serwera DHCP 5.Usługa DNS Działanie DNS

	LAB A: Instalacja serwera DNS Konfigurowanie właściwości usługi serwera DNS LAB B: Konfiguracja serwera DNS Konfigurowanie stref DNS LAB C: Strefy serwera DNS 6.Konfiguracja protokołu Network Time Protocol (NTP) Działanie NTP Konfiguracja protokołu NTP w systemie Windows Konfigurowanie protokołu NTP na urządzeniach Cisco LAB: Konfiguracja protokołu NTP 7.Omówienie zagadnień dot. routingu, translacji adresów, oraz firewall'a Zrozumienie zagadnień routing'u Routing statyczny i dynamiczny Prywatne i publiczne adresy IP Translacja adresów IP (NAT i PAT) Firewall, Windows Firewall LAB: Konfiguracja routingu, translacji adresów oraz firewall'a 8.Konfiguracja usługi VPN Działanie VPN Protokoły i algorytmy w VPN LAB: Przykładowa konfiguracja VPN 9.Konfiguracja usługi IPSec Standard IPSec IPSec: zasady zabezpieczeń IP IPSec: zasady bezpieczeństwa połączeń LAB: Przykładowa konfiguracja usługi IPSec 10.Monitorowanie sieci Monitorowanie sieci Windows Resource Monitor (monitor zasobów) TCPView Wireshark – monitorowanie ruchu sieciowego LAB: Monitorowanie sieci Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Ilość: Szkolenie dla 1 administratora
Szkolenie typ XII	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Wprowadzenie do kursu Wstęp i logistyka szkolenia Cele szkolenia: 2.Wprowadzenie do vSphere i Software Defined Data Center Wyjaśnienie podstawowych pojęć związanych z wirtualizacją Opisanie w jaki sposób vSphere wpasowuje się do Software Defined Data Center oraz infrastruktury opartej na chmurze Wyjaśnienie w jaki sposób vSphere wykorzstuje CPUs, pamięć, sieć oraz dyski Omówienie interfejsów użytkownika vCenter Server oraz hostów ESXi Omówienie architektury hosta ESXi Nawigacja w Direct Console User Interface (DCUI) w celu konfigurowacji hosta ESXi Zapoznanie się z najlepszymi praktykami dotyczącymi zarządzania kontami użytkowników hosta ESXi Instalacja hosta ESXi Używanie VMware Host Client™ w celu dostępu i zarządzania hostem ESXi 3.Maszyny wirtualne Tworzenie i instalacja maszyny wirtualnej Wyjaśnienie znaczenia VMware Tools™ Instalacja VMware Tools™

	Identyfikacja plików tworzących maszynę wirtualną Poznanie komponentów maszyny wirtualnej Omówieni wsparacia dla virtualnych urządzeń maszyny wirtualnej Opis korzyści i przypadki użycia kontenerów Identyfikacja korzyści używania kontenerów 4.vCenter Server Opis architektury vCenter Server Omówienie komunikacji hostów ESXi z vCenter Server Instalacja i konfigurowanie vCenter Server Appliance Używanie vSphere Client do zarządzania zasobami vCenter Server Konfiguracja data center, obiektów organizacyjnych oraz hostów do vCenter Server Zastosowanie ról i uprawnień w celu umożliwienia użytkownikom dostępu do zasobów vCenter Server Tworzenie kopii zapasowej vCenter Server Appliance Monitorowanie vCenter Server pod względem zadań, zdarzeń oraz kondycji Używanie vCenter Server High Availability w celu zabezpieczania vCenter Server Appliance 5.Konfigurowanie i Zarządzanie Wirtualnymi Sieciami Tworzenie i zarządzanie switchami standardowymi Opis rodzajów połączeń do switcha Konfigurowanie zabezpieczeń wirtualnego switcha, zasad ograniczania ruchu i równoważenia obciążenia Porównanie switchy rozproszonych i standardowych w vSphere 6.Konfigurowanie i zarządzanie Pamięcią Masową Identyfikacja protokołów pamięci masowej oraz typów urządzeń Omówienie w jaki sposób hosty ESXi wykorzystują iSCSI, NFS oraz Fibre Channel Tworzenie i zarządzanie systemami plików VMFS i NFS Wyjaśnienie w jaki sposób wielościeżkowość współdziała z iSCSI, NFS oraz Fibre Channel Tworzenie maszyn wirtualnych na systemie plików VMware vSAN™ 7.Zarządzanie Wirtualnymi Maszynami Zastosowanie szablonów oraz klonowania w celu wdrażania nowych maszyn wirtualnych Modyfikowanie i zarządzanie maszynami wirtualnymi Tworzenie Content Library oraz wdrażanie maszyn wirtualnych z szablonów w Content Library Zastosowanie plików specyfikacji w celu poprawienia konfiguracji systemu operacyjnego nowej maszyny wirtualnej Wykonanie migracji vSphere vMotion oraz vSphere Storage vMotion Opis Enhanced vMotion Compatibility Tworzenie i zarządzanie kopii migawkowej maszyny wirtualnej Badanie cech i funkcji VMware vSphere® Replication™ Opis zalet VMware vSphere® Storage API – Data Protection 8.Zarządzanie Zasobami i Monitorowanie Omówienie koncepcji związanych z CPU i pamięcią w środowisku wirtualnym Wyjaśnienie znaczenia ponadwymiarowego wykorzystania zasobów Opis metod optymalizacji CPU i użycia pamięci Zastosowanie różnych narzędzi do monitorowania zużycia zasobów Tworzenie i używanie alarmów do raportowania określonych wartości liczbowych lub zdarzeń 9.Klastry vSphere Opis funkcji klastra vSphere DRS Tworzenie klastra vSphere DRS Monitorowanie konfiguracji klastra Opis opcji tworzenia wysokodostępnego środowiska vSphere Wyjaśnienie budowy vSphere HA Konfigurowanie i zarządzanie klastrem vSphere HA Omówienie cech i funkcji VMware vSphere® Fault Tolerance 10.Skalowalność sieci Konfiguracja i zarządzanie switchami rozproszonymi Opis w jaki sposób VMware vSphere® Network I/O Control podnosi wydajność sieci Wyjaśnienie cech i funkcji switcha rozproszonego takich jak mirroring portów i NetFlow 11.Cykl życia vSphere

	Znaczenie narzędzia vCenter Server Update Planner Opis działania VMware vSphere® Lifecycle Manager™ Zastosowanie vSphere Lifecycle Manager do aktualizowania hostów ESXi w klastrze Sprawdzanie zgodności hosta ESXi przy użyciu obrazu klastra Opis zaktualizacji VMware Tools i VM Hardware 12.Skalowalność hosta i zarządzania Używanie profili hostów do zarządzania zgodnością konfiguracji ESXi Tworzenie i zarządzanie pulami zasobów w klastrze Opis działania skalowalnością zasobów 13.Skalowalność pamięci masowej Wyjaśnienie, dlaczego VMware vSphere® VMFS jest wysokowydajnym, skalowalnym systemem plików Wyjaśnienie działania VMware vSphere® Storage APIs - Array Integration, VMware vSphere® API for StorageAwareness™ oraz vSphere APIs for I/O Filtering Konfiguracja i przypisywanie polityk storage'owych do maszyn wirtualnych Tworzenie polityk storage'owych dla VMware vSAN™ Rozpoznawanie komponentów i architektura vSphere Virtual Volumes Konfiguracja VMware vSphere® Storage DRS™ oraz VMware vSphere® Storage I/O Control Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - Uczestnik po zakończeniu szkolenia musi mieć możliwość przystąpienia do certyfikowanego egzaminu za dodatkową opłatą np. w centrum PearsonVUE lub online Ilość: Szkolenie dla 1 administratora
Szkolenie typ XIII	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Wprowadzenie do kursu Wstęp i logistyka szkolenia Cele szkolenia 2.Wprowadzenie do vSphere i Software Defined Data Center Wyjaśnienie podstawowych pojęć związanych z wirtualizacją Opisanie w jaki sposób vSphere wpasowuje się do Software Defined Data Center oraz infrastruktury opartej na chmurze Wyjaśnienie w jaki sposób vSphere wykorzstuje CPUs, pamięć, sieć oraz dyski Omówienie interfejsów użytkownika vCenter Server oraz hostów ESXi Omówienie architektury hosta ESXi Nawigacja w Direct Console User Interface (DCUI) w celu konfigurowacji hosta ESXi Zapoznanie się z najlepszymi praktykami dotyczącymi zarządzania kontami użytkowników hosta ESXi Instalacja hosta ESXi Używanie VMware Host Client™ w celu dostępu i zarządzania hostem ESXi 3.Maszyny wirtualne Tworzenie i instalacja maszyny wirtualnej Wyjaśnienie znaczenia VMware Tools™ Instalacja VMware Tools™ Identyfikacja plików tworzących maszynę wirtualną Poznanie komponentów maszyny wirtualnej Omówieni wsparacia dla virtualnych urządzeń maszyny wirtualnej Opis korzyści i przypadki użycia kontenerów Identyfikacja korzyści używania kontenerów 4.vCenter Server Opis architektury vCenter Server Omówienie komunikacji hostów ESXi z vCenter Server Instalacja i konfigurowanie vCenter Server Appliance Używanie vSphere Client do zarządzania zasobami vCenter Server Konfiguracja data center, obiektów organizacyjnych oraz hostów do vCenter Server

	Zastosowanie ról i uprawnień w celu umożliwienia użytkownikom dostępu do zasobów vCenter Server Tworzenie kopii zapasowej vCenter Server Appliance Monitorowanie vCenter Server pod względem zadań, zdarzeń oraz kondycji Używanie vCenter Server High Availability w celu zabezpieczania vCenter Server Appliance 5.Konfigurowanie i Zarządzanie Wirtualnymi Sieciami Tworzenie i zarządzanie switchami standardowymi Opis rodzajów połączeń do switcha Konfigurowanie zabezpieczeń wirtualnego switcha, zasad ograniczania ruchu i równoważenia obciążenia Porównanie switchy rozproszonych i standardowych w vSphere 6.Konfigurowanie i zarządzanie Pamięcią Masową Identyfikacja protokołów pamięci masowej oraz typów urządzeń Omówienie w jaki sposób hosty ESXi wykorzystują iSCSI, NFS oraz Fibre Channel Tworzenie i zarządzanie systemami plików VMFS i NFS Wyjaśnienie w jaki sposób wielościeżkowość współdziała z iSCSI, NFS oraz Fibre Channel Tworzenie maszyn wirtualnych na systemie plików VMware vSAN™ 7.Zarządzanie Wirtualnymi Maszynami Zastosowanie szablonów oraz klonowania w celu wdrażania nowych maszyn wirtualnych Modyfikowanie i zarządzanie maszynami wirtualnymi Tworzenie Content Library oraz wdrażanie maszyn wirtualnych z szablonów w Content Library Zastosowanie plików specyfikacji w celu poprawienia konfiguracji systemu operacyjnego nowej maszyny wirtualnej Wykonanie migracji vSphere vMotion oraz vSphere Storage vMotion Opis Enhanced vMotion Compatibility Tworzenie i zarządzanie kopii migawkowej maszyny wirtualnej Badanie cech i funkcji VMware vSphere® Replication™ Opis zalet VMware vSphere® Storage API – Data Protection 8.Zarządzanie Zasobami i Monitorowanie Omówienie koncepcji związanych z CPU i pamięcią w środowisku wirtualnym Wyjaśnienie znaczenia ponadwymiarowego wykorzystania zasobów Opis metod optymalizacji CPU i użycia pamięci Zastosowanie różnych narzędzi do monitorowania zużycia zasobów Tworzenie i używanie alarmów do raportowania określonych wartości liczbowych lub zdarzeń 9.Klastry vSphere Opis funkcji klastra vSphere DRS Tworzenie klastra vSphere DRS Monitorowanie konfiguracji klastra Opis opcji tworzenia wysokodostępnego środowiska vSphere Wyjaśnienie budowy vSphere HA Konfigurowanie i zarządzanie klastrem vSphere HA Omówienie cech i funkcji VMware vSphere® Fault Tolerance 10.Cykl życia vSphere Znaczenie narzędzia vCenter Server Update Planner Opis działania VMware vSphere® Lifecycle Manager™ Zastosowanie vSphere Lifecycle Manager do aktualizowania hostów ESXi w klastrze Sprawdzanie zgodności hosta ESXi przy użyciu obrazu klastra Opis zaktualizacji VMware Tools i VM Hardware Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - Uczestnik po zakończeniu szkolenia musi mieć możliwość przystąpienia do certyfikowanego egzaminu za dodatkową opłatą w centrum PearsonVUE lub są również dostępne w formule online Ilość: Szkolenie dla 1 administratora
Szkolenie typ XIV	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych

	Program szkolenia – zakres minimalny: 1.Docker Architektura i instalacja Budowanie i zarządzanie obrazami, repozytoria Praca z kontenerami Projektowanie wielokontenerowych aplikacji 2.Kubernetes Orkiestracja, wstęp teoretyczny Instalacja Kubernetes, zarządzanie klastrem Omówienie obiektów występujących w Kubernetes Praca z klastrem za pomocą CLI Zapoznanie z WEB UI Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby szkolenie zostało przeprowadzone metodą zdalną. Ilość: Szkolenie dla 1 administratora
Szkolenie typ XV	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Docker teoria Przykładowe zastosowania Główne komponenty Architektura 2.Instalacja Dockera Windows Pro/Enterprise / MacOS Debian 3.Praca z Dockerem - wiersz poleceń Obrazy Repozytorium Uruchamianie kontenerów Otwarcie kontenerów na ruch zewnętrzny Zasoby dyskowe 4.Praca z Dockerem - Dockerfile Tworzenie pliku Dockerfile Omówienie składni Budowa obrazu Praca z tagami i repozytorium Rozszerzanie obrazów 5.Praca z Dockerem - docker–compose Tworzenie pliku docker-compose.yml Omówienie składni Montowanie zasobów dyskowych Konfiguracja sieci 6.Wzorce projektowe 7.Wstęp do orkiestracji Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Ilość: Szkolenie dla 1 administratora
Szkolenie typ XVI	Szkolenie zdalne dla administratora z zakresu posiadanego przez Zamawiającego oprogramowania i systemów operacyjnych Program szkolenia – zakres minimalny: 1.Wprowadzenie Architektura klastra Główne komponenty i ich zadania Sposób wdrożenia aplikacji, rola kontrolerów w utrzymaniu stanu klastra

	2.Budowa klastra Kubernetes Wdrażanie Control Plane Wdrażanie Worker Nodes 3.Praca z Kubernetes Polecenie kubectl Konfigurowanie kontekstów i przełączanie się pomiędzy nimi Podział klastra - namespaces 4.Podstawowe obiekty Pod Namespace Job CronJob ConfigMap Secrets 5.Kontrolery ReplicaSet Deployment DaemonSet StatefulSet 6.Skalowanie aplikacji w klastrze RollingUpdate – skalowanie góra-dół Przywracanie poprzedniej wersji aplikacji Skalowanie w poziomie 7.Sieć Kubernetesa Rola coreDNS Wystawianie aplikacji na zewnątrz klastra Obiekt Service i jego rodzaje 8.Przechowywanie danych emptyDir HostPath PersistentVolume PersistentVolumeClaim StorageClass, Storage Class Interface, 9.Helm Pliki charts Instalacja i deinstalacja aplikacji za pomocą Helm Repozytoria 10.Ingress zasób Ingress i Ingress kontroler 11.Dashboard – dostęp do klastra przez www Instalacja dashboard 12.Elementy bezpieczeństwa klastra – podstawowe wiadomości Network Policy RBAC Role, ClusterRole i RoleBinding Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Ilość: Szkolenie dla 1 administratora

Szkolenia dla pracowników z zakresu cyberbezpieczeństwa oraz dostarczonego oprogramowania

Nazwa	Minimalne wymagania dla szkoleń
Szkolenia dla pracowników z	Szkolenie zdalne dla pracowników z zakresu cyberbezpieczeństwa

zakresu cyberbezpieczeństwa	Program szkolenia – zakres minimalny: Czym jest cyberbezpieczeństwo. Podstawowe przedstawienie zagadnienia cyberbezpieczenstwa Przedstawienie zagrożeń, które czyhają na nas w sieci (rodzaje zagrożeń i ich konsekwencje) Opis i wymagania normy ISO/IEC 27001 Dlaczego wiedza o cyberbezpieczeństwie jest konieczna? Sposoby ochrony kont i danych przed potencjalnym zagrożeniem. Częsta zmiana haseł, czy ustalanie ich odpowiedniej trudności a co za tym idzie programy pomagające w tym (np. keypas) Logowanie w sieci. Opis Certyfikatów stron internetowych. Darmowe WiFi i automatyczne podłączanie się. Praca zdalna - czym jest VPN i jak z niego korzystać. Wprowadzenie do sieci komputerowych - niebezpieczeństwo sieci otwartych bezprzewodowych. Niezabezpieczone protokoły sieciowe - HTTP FTP Zaszyfrowana komunikacja w Internecie (Signal i WhatsApp) Ochrona plików i dysków czyli podstawy szyfrowania. Przedstawienie przykładów i nauka rozpoznawania niepożądanych maili i ich zawartości. Odpowiednia weryfikacja odbiorcy i nadawcy. Weryfikacją wiadomości e-mail Weryfikacja i skan plików znajdujących się w załączniku. Przykłady ataków oraz sposoby na ochronę przed nimi pod kątem zwykłego użytkownika Phishing i td - Sposoby na zabezpieczenie się przed włamaniami i oszustwem w sieci Programy antywirusowe i ich rola (omówienie popularnych programów i opis ich działania) Tworzenie kopii zapasowych i ich odzyskiwanie po awarii. Sposoby tworzenia backup'ów. Podpis elektroniczny dokumentów w prosty i bezpieczny sposób. Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - Uczestnik po zakończeniu szkolenia musi mieć możliwość przystąpienia do certyfikowanego egzaminu Ilość: Szkolenie dla maksymalnie 100 pracowników	
Szkolenia dla pracowników z zakresu dostarczonego oprogramowania	**Szkolenie typ I**	Szkolenie zdalne dla pracowników z zakresu posiadanego przez Zamawiającego oprogramowania Program szkolenia – zakres minimalny: 1.Omówienie podstaw chmury Omówienie Cloud Computing Usługi Microsoft Cloud Migracja do usług w chmurze 2.Podstawy usługi Microsoft 365 Usługi podstawowe Microsoft 365 Usługi lokalne firmy Microsoft a usługi chmurowe Microsoft 365 Enterprise Mobility w Microsoft 365 Współpraca w Microsoft 365 3.Bezpieczeństwo, zgodność, prywatność i zaufanie w usłudze Microsoft 365 Przegląd zabezpieczeń organizacji Podstawy tożsamości Urządzenia i ochrona danych Zgodność z Microsoft 365 4.Subskrypcje i wsparcie w Microsoft 365 Subskrypcje, licencje i płatności Microsoft 365 Wsparcie w Microsoft 365 Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną

		- Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby: - Szkolenie zdalne - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - Uczestnik po zakończeniu szkolenia musi mieć możliwość przystąpienia do certyfikowanego egzaminu Microsoft Ilość: Szkolenie dla 1 administratora
	Szkolenie typ II	Szkolenie zdalne dla pracowników z zakresu posiadanego przez Zamawiającego oprogramowania Program szkolenia – zakres minimalny: 1. Planowanie i obsługa administracyjna Office 365 Omówienie usługi Office 365 Aprowizacja dzierżawy Office 365 Planowanie wdrożenia pilotażowego. 2. Zarządzanie użytkownikami i grupami Office 365 Zarządzanie kontami użytkowników i licencjami Zarządzanie hasłami i uwierzytelnianiem Zarządzanie grupami zabezpieczeń w Office 365 Zarządzanie użytkownikami i grupami Office 365 za pomocą Windows PowerShell Konfigurowanie dostępu administracyjnego. 3. Konfigurowanie łączności klienta z Microsoft Office 365 Planowanie dla klientów Office 365 Planowanie łączności dla klientów Office 365 Konfigurowanie łączności dla klientów Office 365. 4. Planowanie i konfigurowanie synchronizacji katalogów Planowanie i przygotowanie do synchronizacji katalogów Wdrażanie synchronizacji katalogów za pomocą usługi Azure AD Connect Zarządzanie tożsamościami Office 365 z synchronizacją katalogów 5. Planowanie i wdrażanie Office 365 ProPlus: Omówienie usługi Office 365 ProPlus Planowanie wdrożeń Office 365 ProPlus i zarządzanie nimi Planowanie i zarządzanie scentralizowanymi wdrożeniami Office 365 ProPlus Telemetria i raportowanie 6. Planowanie i zarządzanie adresatami i uprawnieniami Exchange Online Omówienie usługi Exchange Online Zarządzanie adresatami Exchange Online Planowanie i konfiguracja uprawnień Exchange Online 7. Planowanie i konfigurowanie usług Exchange Online Planowanie i konfigurowanie przepływu wiadomości e-mail w Office 365 Planowanie i konfigurowanie ochrony poczty e-mail w Office 365 Planowanie i konfigurowanie zasad dostępu klienta Migracja do Exchange Online 8. Planowanie i wdrażanie Microsoft Teams Omówienie zespołów Wdrażanie zespołów Uwierzytelnianie i dostęp Przenoszenie Skype dla firm do Microsoft Teams Zarządzanie i raportowanie 9. Planowanie i konfigurowanie SharePoint Online Konfigurowanie usług SharePoint Online Planowanie i konfigurowanie zbiorów witryn SharePoint Online Planowanie i konfigurowanie zewnętrznego udostępniania użytkowników 10. Planowanie i konfigurowanie rozwiązania współpracy Office 365

		Planowanie i zarządzanie Yammer Enterprise Planowanie i konfigurowanie OneDrive dla Firm Konfigurowanie grup Office 365 11. Planowanie i konfigurowanie bezpieczeństwa i zgodności w Office 365 Omówienie funkcji zgodności w Office 365 Planowanie i konfigurowanie usługi Azure Information Protection w Office 365 Zarządzanie funkcjami zgodności w Office 365 12. Monitorowanie i rozwiązywanie problemów z Microsoft Office 365 Rozwiązywanie problemów z Office 365 Monitorowanie kondycji usługi Office 365 Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby: - Szkolenie zdalne - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - Uczestnik po zakończeniu szkolenia musi mieć możliwość przystąpienia do certyfikowanego egzaminu Microsoft Ilość: Szkolenie dla 1 administratora
	Szkolenie typ III	Szkolenie zdalne dla pracowników z zakresu posiadanego przez Zamawiającego oprogramowania Program szkolenia – zakres minimalny: 1.Omówienie Microsoft Teams Omówienie zespołów Microsoft Przegląd bezpieczeństwa i zgodności w Microsoft Teams Omówienie zarządzania zespołami Microsoft 2.Wdrażanie zarządzania, bezpieczeństwa i zgodności z Microsoft Teams Wdrożenie zarządzania i zarządzania cyklem życia dla zespołów Microsoft Wdrażanie zabezpieczeń dla zespołów Microsoft Wdrażanie zgodności dla zespołów Microsoft 3.Przygotowanie środowisko do wdrożenia Microsoft Teams Uaktualnienie programu Skype dla firm do Microsoft Teams Planowanie i konfiguracja ustawień sieciowych dla Microsoft Teams Wdrażanie punktów końcowych Microsoft Teams i ich zarządzanie 4.Wdrażanie zespołów i zarządzanie nimi Tworzenie zespołów i ich zarządzanie Zarządzanie członkostwem Zarządzanie dostępem dla użytkowników zewnętrznych 5.Zarządzanie współpracą w Microsoft Teams: Zarządzanie czatami i doświadczeniami współpracy Zarządzanie ustawieniami aplikacji Teams 6.Zarządzanie komunikacją w Microsoft Teams Zarządzanie wydarzeniami na żywo i doświadczeniami ze spotkań Zarządzanie numerami telefonów Zarządzanie systemem telefonicznym dla zespołów Microsoft Problemy z dźwiękiem, wideo i problemy z klientem Wymagania dodatkowe: - Szkolenie powinno zostać przeprowadzone metodą zdalną - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych Wymagania dodatkowe: W ramach realizacji szkolenia wymagane jest, aby:

		- Szkolenie zdalne - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych - Uczestnik po zakończeniu szkolenia musi mieć możliwość przystąpienia do certyfikowanego egzaminu Microsoft Ilość: Szkolenie dla 1 administratora

Część III Przedmiotu zamówienia

Diagnoza 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. 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 – Wykonawca ma obowiązek na udzielenie informacji na temat audytowanych elementów wynikających z raportu w terminie maksymalnie 7 dni od wykonania 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