



OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup sprzętu komputerowego i oprogramowania w ramach projektu „Poprawa cyberbezpieczeństwa w Urzędzie Gminy Skórzec”

realizowanego w ramach konkursu grantowego „Cyberbezpieczny Samorząd”
w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027,
Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Skórzec, luty 2026 r.

Spis treści

1	OGÓLNE INFORMACJE.....	3
2	WYMAGANIA OGÓLNE.....	5
3	SERWER – 3 SZT.	5
4	SERWEROWY SYSTEM OPERACYJNY – 3 SZT.....	11
5	UTM – 2 SZT.	13
6	ZARZĄDZANY PRZEŁĄCZNIK SIECIOWY – 2 SZT.....	21
7	URZĄDZENIE PAMIĘCI MASOWEJ – TYP I – 1 SZT.	21
8	URZĄDZENIE PAMIĘCI MASOWEJ – TYP II – 1 SZT.	25
9	UPS – 2 SZT.....	26
10	SPRZĘTOWY KLUCZ BEZPIECZEŃSTWA – 20 SZT.	27
11	OPROGRAMOWANIE TYPU CMDDB I SAM – 1 KPL.....	28
12	OPROGRAMOWANIE KLASY EDR – 1 KPL.	37
13	OPROGRAMOWANIE DO ARCHIWIZACJI – 1 KPL.	38
14	OPROGRAMOWANIE DO WIRTUALIZACJI – 1 KPL.	39
15	INSTALACJA, MIGRACJA, WDROŻENIE – 1 KPL.	41
16	KURSY INFORMATYCZNE ONLINE – 1 KPL.	42

1 Ogólne informacje

Niniejsze Zamówienie jest częścią projektu finansowanego ze środków funduszy UE pn.: „Poprawa cyberbezpieczeństwa w Urzędzie Gminy Skórzec”, który realizowany jest przez Gminę Skórzec w ramach konkursu grantowego „Cyberbezpieczny Samorząd” w ramach Funduszu Europejskiego na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Głównym miejscem realizacji Zamówienia będzie Urząd Gminy Skórzec, ul. Siedlecka 3, 08-114 Skórzec.

Przedmiot niniejszego zamówienia obejmuje dostarczenie poniższego sprzętu i oprogramowania wraz z ich instalacją i konfiguracją oraz dostępem do platformy szkoleniowej dla pracowników Urzędu Gminy:

1. Serwer – 3 szt.
2. Serwerowy system operacyjny – 3 szt.
3. UTM – 2 szt.
4. Zarządzany przełącznik sieciowy – 2 szt.
5. Urządzenie pamięci masowej – typ I – 1 szt.
6. Urządzenie pamięci masowej – typ II – 1 szt.
7. UPS – 2 szt.
8. Sprzętowy klucz bezpieczeństwa – 20 szt.
9. Oprogramowanie typu CMDB i sAM – 1 kpl.
10. Oprogramowanie klasy EDR – 1 kpl.
11. Oprogramowanie do archiwizacji – 1 kpl.
12. Oprogramowanie do wirtualizacji – 1 kpl.
13. Instalacja, migracja, wdrożenie – 1 kpl.
14. Kursy informatyczne online – 1 kpl.

TERMIN REALIZACJI

Wymagany termin wykonania Zamówienia – **60 dni kalendarzowych od dnia podpisania umowy.**

Opisane poniżej wymagania stanowią zakres minimalnych oczekiwań Zamawiającego dla przedmiotu zamówienia.

OGÓLNE ZASADY RÓWNOWAŻNOŚCI ROZWIĄZAŃ:

1. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, z tym zastrzeżeniem, że nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu

równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są przeznaczone. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

2. Wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo zamówień publicznych, Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający informuje, że w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy, jakie cechy powinny posiadać składniki użyte do realizacji przedmiotu zamówienia. Zamawiający zgodnie z art. 99 ust. 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, zwanej dalej ustawą, dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.), jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach.
3. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia, dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania.

2 Wymagania ogólne

Lp.	Minimalne wymagania
1.	<p>a) Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.</p> <p>b) Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.</p> <p>c) Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.</p> <p>d) W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia.</p> <p>e) Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.</p> <p>f) Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.</p> <p>g) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji w dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.</p> <p>h) Gwarancja i serwis na urządzenia musi być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku gdy Oferent nie posiada takiej autoryzacji.</p> <p>i) Urządzenia na etapie dostarczenia Producent => Zamawiający nie mogą podlegać modyfikacjom.</p> <p>j) Zamawiający wymaga możliwości sprawdzenia statusu gwarancji i konfiguracji oferowanego sprzętu na stronie producenta po podaniu jego numeru seryjnego, strona producenta musi być podstroną głównej domeny producenta sprzętu.</p> <p>k) Na min. 3 dni przed dostawą sprzętu należy przesłać Zamawiającemu wykaz numerów seryjnych oferowanych urządzeń celem weryfikacji u producenta.</p> <p>l) Wymagana ogólnopolska, telefoniczna infolinia/linia techniczna producenta w języku polskim (ogólnopolski numer o zredukowanej odpłatności 0-800 lub 0-801).</p> <p>m) Zamawiający wymaga, aby serwer był wyprodukowany w UE i pochodził z oficjalnego kanału dystrybucyjnego w Polsce.</p> <p>n) Przed dostawą Wykonawca ma obowiązek dołączyć pisemne oświadczenie producenta potwierdzające pochodzenie elementów serwerów oraz kompletnej macierzy z oficjalnego kanału dystrybucyjnego w Polsce.</p>

3 Serwer – 3 szt.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Obudowa	1. Obudowa Rack o wysokości max 1U.

		<p>2. Możliwość instalacji minimum 8 dysków 2.5".</p> <p>3. Możliwość instalacji dysków SAS/SATA/NVMe.</p> <p>4. Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy..</p>
2.	Płyta główna	<p>1. Możliwość obsługi procesorów min. 64 rdzeniowych</p> <p>2. Płyta główna musi być zaprojektowana przez producenta i oznaczona jego znakiem firmowym.</p> <p>3. Na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci.</p> <p>4. Płyta główna powinna obsługiwać do 3TB pamięci RAM.</p>
3.	Procesor	<p>Zainstalowany procesor min. 16-rdzeniowy, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 170 pkt w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocessorowej.</p> <p><u>Wydruk ze strony potwierdzający osiągany wynik dołączyć do oferty.</u></p>
4.	RAM	Zainstalowane min. 64GB
5.	Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
6.	Dyski twarde	<p>1. Zainstalowane min. 2 x dysk SSD o pojemności min. 480GB, 6Gbps, Hot-Plug, 1 DWPD;</p> <p>2. Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1.</p>
7.	Gniazda PCI	Minimum trzy sloty PCIe, w tym min. 2x8 i min. 1x16
8.	Interfejsy sieciowe/FC/SAS	<p>1. Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe).</p> <p>2. Karta PCIe Low Profile wyposażona w minimum 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT.</p>
9.	Wbudowane porty	<p>1. min. 4 porty USB w tym:</p> <ul style="list-style-type: none"> ○ min. 1 port USB 3.0 z tyłu obudowy, ○ min. 1 port micro USB z przodu obudowy <p>2. min. 2 porty VGA z czego jeden z przodu obudowy.</p> <p>3. Możliwość rozbudowy o port RS232.</p>
10.	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
11.	Wentylatory	Redundantne
12.	Zasilanie	<p>1. Minimum dwa redundantne zasilacze o mocy minimum 700W z certyfikatem minimum Titanium.</p> <p>2. 2 x przewód C13/C14 o długości minimum 2 metry.</p>
13.	Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
14.	Bezpieczeństwo	<p>1. Zatrzaśk górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</p> <p>2. Moduł TPM 2.0.</p> <p>3. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</p> <p>4. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.</p>

		<p>5. Możliwość dynamicznego włączania i wyłączenia portów USB na obudowie – bez potrzeby restartu serwera.</p> <p>6. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.</p>
15.	Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</p> <ol style="list-style-type: none"> 1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3) szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; 4) możliwość podmontowania zdalnych wirtualnych napędów; 5) wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 6) możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 7) integracja z Active Directory; 8) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 9) możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera.
16.	Oprogramowanie do zarządzania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ol style="list-style-type: none"> 1) Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; 2) Integracja z Active Directory; 3) Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; 4) Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish; 5) Możliwość eksportu raportu do CSV, HTML, XLS, PDF; 6) Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu; 7) Grupowanie urządzeń w oparciu o kryteria użytkownika; 8) Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach; 9) Szybki podgląd stanu środowiska; 10) Podsumowanie stanu dla każdego urządzenia; 11) Szczegółowy status urządzenia/elementu/komponentu; 12) Generowanie alertów przy zmianie stanu urządzenia; 13) Filtry raportów umożliwiające podgląd najważniejszych zdarzeń; 14) Możliwość przejęcia zdalnego pulpitu; 15) Możliwość podmontowania wirtualnego napędu; 16) Możliwość definiowania ról administratorów; 17) Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów; 18) Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta; 19) Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; 20) Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego,

		<p>obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera;</p> <p>21) Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności;</p> <p>22) Zdalne uruchamianie diagnostyki serwera;</p> <p>23) Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</p> <p>24) Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</p>
17.	Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <p>1) Monitoring:</p> <ul style="list-style-type: none"> • ilość podłączonych oraz rozłączonych systemów • stan podłączonych urządzeń • informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów • Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia • informacje o statusie gwarancji dla poszczególnych urządzeń • informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń • informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. • Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych • Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. • Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. • Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. • Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. • Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> ○ Obciążeniu procesora ○ Zużyciu pamięci RAM ○ Temperaturze procesorów ○ Temperaturze powietrza wlotowego ○ Zużyciu prądu ○ Zmianach w fizycznej konfiguracji serwera ○ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Monitoring parametrów pamięci masowych z informacją o minimum:

	<ul style="list-style-type: none"> ○ Opóźnieniach ○ IOPS ○ Przepustowości ○ Utylizacji kontrolerów ○ Pojemność całkowita i dostępna ○ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ○ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. <p>2) Aktualizacja firmware</p> <ul style="list-style-type: none"> • Możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania; • Możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania; • Możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania <p>3) Raporty</p> <ul style="list-style-type: none"> • Możliwość generowania raportów dla serwerów zawierających informację o: nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej; • Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji. • Generowanie raportów do plików CSV i PDF. <p>4) Cyberbezpieczeństwo</p> <ul style="list-style-type: none"> • Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. • Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. • Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. • Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. <p>5) Wspierane urządzenia</p> <ul style="list-style-type: none"> • Urządzenie Producenta dostarczane w ramach postępowania • Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) <p>6) Wirtualny asystent</p> <ul style="list-style-type: none"> • Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury.
--	---

		<p>7) Możliwość rozszerzenia funkcjonalności</p> <ul style="list-style-type: none"> Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. <p>8) Inne</p> <ul style="list-style-type: none"> Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android.
18.	Certyfikaty	<p>1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-50001 oraz ISO-14001.</p> <p>2. Serwer musi posiadać deklarację CE.</p> <p>3. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. <u>Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku, załączony do oferty przez Wykonawcę.</u></p>
19.	Dokumentacja użytkownika	<p>1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
20.	Warunki gwarancji (Kryterium punktowe)	<p>1) Gwarancja producenta: min. 36 miesięcy lub dłużej zgodnie ze złożoną ofertą.</p> <p>2) Czas reakcji serwisu następnego dnia roboczego.</p> <p>3) Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie lub przez Internet</p> <p>4) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</p> <p>5) Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:</p> <ul style="list-style-type: none"> Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu

		<p>pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.</p> <p>6) <u>Wymagane dołączenie do oferty oświadczenia Wykonawcy lub Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</u></p> <p>7) W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – <u>wymagane jest dołączenie do oferty oświadczenia podmiotu wykonującego Serwis lub Producenta potwierdzające powyższe.</u></p> <p>8) Firma serwisująca musi posiadać ISO9001 oraz ISO27001 na świadczenie usług serwisowych oraz posiada autoryzację producenta urządzeń – <u>dokumenty potwierdzające należy załączyć do oferty.</u></p>
--	--	---

4 Serwerowy system operacyjny – 3 szt.

LP.	WYMAGANIA MINIMALNE
1.	<p>Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:</p> <ol style="list-style-type: none"> 1) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i minimum dwóch licencjonowanych wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji z odpowiednią ilością rdzeni procesora. 2) Możliwość wykorzystania minimum 128 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 3) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 9) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 10) Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ul style="list-style-type: none"> – pozwalają na zmianę rozmiaru w czasie pracy systemu, – umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, – umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, – umożliwiają zdefiniowanie list kontroli dostępu (ACL). 11) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 12) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

- 13) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
- 14) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- 15) Wbudowana zaporą internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- 16) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
- 17) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
- 18) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
- 19) Mechanizmy logowania w oparciu o:
 - Login i hasło,
 - Karty z certyfikatami (smartcard),
 - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- 20) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
- 21) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- 22) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- 23) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- 24) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
- 25) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- 26) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - 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:
 - a. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - b. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - c. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - d. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
 - e. Zdalna dystrybucja oprogramowania na stacje robocze.
 - f. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej;
 - g. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:
 - i. Dystrybucję certyfikatów poprzez http

	<ul style="list-style-type: none"> ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domeny, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. <ul style="list-style-type: none"> – Szyfrowanie plików i folderów. – Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). – Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. – Serwis udostępniania stron WWW. – Wsparcie dla protokołu IP w wersji 6 (IPv6), – Wsparcie dla algorytmów Suite B (RFC 4869), – Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, – 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: <ul style="list-style-type: none"> i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode). – Wbudowane mechanizmy pamięci masowej, które umożliwią łączenie wewnętrznych dysków pamięci w klastrze serwerów fizycznych (od 2 do maksymalnie 16) w pulę pamięci masowej zdefiniowaną programowo (SDS). <p>27) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p> <p>28) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p> <p>29) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>30) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>31) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p> <p>32) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.</p> <p>33) System musi być w najnowszej wersji na dzień publikacji ogłoszenia o zamówieniu publicznym.</p>
2.	Wraz z Serwerowym Systemem Operacyjnym wymagane jest dostarczenie 40 licencji CAL na użytkownika.

5 UTM – 2 szt.

LP.	OPIS	WYMAGANIA MINIMALNE
-----	------	---------------------

1.	Wymagania ogólne	<ol style="list-style-type: none"> 1) Urządzenie powinno zostać dostarczone w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. 2) Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2. 3) Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) 4) Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie HA Active-Passive lub Active-Active. 5) System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. 6) Rozwiązanie musi być wyposażone w co najmniej jeden wbudowany dysk SSD służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu. 7) Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy 8) Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB) 9) Rozwiązanie umożliwiające podłączenie modemów sieci komórkowych produkowanych przez firmy trzecie. 10) Możliwość przeprowadzenie konfiguracji w trybie Zero Touch. 11) Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowych. 12) Pamięć operacyjna RAM nie mniej niż: 8GB DDR4 13) Przestrzeń do przechowywania logów i raportów nie mniej niż: 64GB. 14) Liczba fizycznych interfejsów minimum gigabitowych nie mniej niż: 6 szt. 15) Liczba fizycznych interfejsów SFP+ nie mniej niż: 2szt. 16) Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż: 128
2.	Wydajność	<ol style="list-style-type: none"> 1) Wydajność Firewall nie mniej niż (Gbps): 11 2) Wydajność Firewall IMIX nie mniej niż (Gbps): 6 3) Wydajność IPS nie mniej niż (Gbps): 4 4) Wydajność FW+IPS+AV nie mniej niż (Gbps): 3 5) Wydajność NGFW nie mniej niż (Gbps): 3 6) Liczba równoczesnych połączeń nie mniejsza niż: 6 000 000 7) Liczba nowych połączeń na sekundę nie mniejsza niż: 73 000 8) Wydajność IPsec VPN nie mniej niż (Gbps): 6 9) Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Gbps): 0,9 10) Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: 18 000 11) Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: 1000 12) Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż: 2000
3.	Zarządzanie	<ol style="list-style-type: none"> 1) Rozwiązanie powinno być zarządzane przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. 2) Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). 3) Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. 4) Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia

	<p>diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter.</p> <p>5) Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.</p> <p>6) Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administratora, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów.</p> <p>7) Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.</p> <p>8) System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności.</p> <p>9) System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.</p> <p>10) System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.</p> <p>11) Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).</p> <p>12) System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polityki bezpieczeństwa.</p> <p>13) Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm).</p> <p>14) System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog).</p> <p>15) Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.</p> <p>16) System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).</p> <p>17) Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta.</p> <p>18) System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednika).</p> <p>19) System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.</p> <p>20) System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta, przy czym w podstawowej wersji utrzymywany i udostępniany jest on bezpłatnie i nie wymaga zakupu osobnych subskrypcji.</p> <p>21) Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, via email jak i dodatkowo do centralnego systemu zarządzania w chmurze.</p>
--	---

		<p>22) Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.</p> <p>23) Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.</p> <p>24) Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.</p> <p>25) Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.</p> <p>26) Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI.</p> <p>27) Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixes, przy czym administrator powinien móc funkcjonalność tą wyłączyć.</p> <p>28) Rozwiązanie powinno oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konfiguracji urządzenia. Dane powinny być zabezpieczone dedykowanym kluczem szyfrującym tworzonym na podstawie bezpiecznie składowanego poza urządzeniem hasła.</p> <p>29) Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych.</p>
4.	Zapora sieciowa	<p>1) Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection.</p> <p>2) System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.</p> <p>3) Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.</p> <p>4) System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.</p> <p>5) System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania).</p> <p>6) System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę.</p> <p>7) Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.</p> <p>8) System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN.</p> <p>9) Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.</p> <p>10) System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (glokalizacja IP).</p> <p>11) Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina.</p> <p>12) System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.</p>

5.	Trasowanie ruchu	<ol style="list-style-type: none"> 1) Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. 2) Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 3) Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. 4) Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN. 5) Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast. 6) Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). 7) Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). 8) Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.
6.	Translacja adresów i portów	<ol style="list-style-type: none"> 1) Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. 2) Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT. 3) Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule.
7.	Kształtowanie pasma i jakość usług	<ol style="list-style-type: none"> 1) System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji. 2) Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. 3) System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. 4) Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. 5) Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet (od 1 Business Critical do 7 Best Effort).
8.	Pozostałe	<ol style="list-style-type: none"> 1) System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 2) Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. 3) Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). 4) System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. 5) System powinien oferować wsparcie dla IEEE 802.1Q VLAN z możliwością konfiguracji niezależnych puli DHCP. 6) Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 7) System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. 8) Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4,

		<p>4in6 oraz IPv6 rapid deployment (6rd).</p> <p>9) Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).</p> <p>10) Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.</p>
9.	Uwierzytelnianie i obsługa użytkowników	<p>1) Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.</p> <p>2) Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników.</p> <p>3) System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.</p> <p>4) Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.</p> <p>5) System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).</p> <p>6) Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server.</p> <p>7) System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.</p> <p>8) Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.</p> <p>9) Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania.</p> <p>10) Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS.</p> <p>11) Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.</p> <p>12) Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.</p>
10.	Koncentrator VPN	<p>1) System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.</p> <p>2) System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519).</p> <p>3) System musi obsługiwać połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN.</p> <p>4) Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN.</p> <p>5) Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback.</p> <p>6) Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego.</p> <p>7) Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth.</p> <p>8) Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.</p> <p>9) Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia</p>

		<p>realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.</p> <p>10) Urządzenie musi obsługiwać połączenia L2TP over IPsec.</p> <p>11) Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej.</p>
11.	Logowanie i raportowanie	<p>1) System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym.</p> <p>2) System powinien umożliwiać składowanie oraz archiwizację logów.</p> <p>3) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.</p> <p>4) Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.</p> <p>5) Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa</p> <p>6) System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.</p> <p>7) System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.</p> <p>8) Rozwiązanie powinno umożliwiać wysyłanie raportów via email.</p> <p>9) Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV.</p> <p>10) Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.</p> <p>11) System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.</p> <p>12) System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.</p> <p>13) Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.</p> <p>14) System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.</p>
12.	Intrusion Prevention System i Advanced Threat Protection	<p>1) Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur.</p> <p>2) Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.</p> <p>3) Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS.</p> <p>4) Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.</p> <p>5) System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.</p>
13.	Ochrona i kontrola web	<p>1) Ochrona przez Malware</p> <ul style="list-style-type: none"> -Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. -Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. -Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. -Wymagane jest, aby system automatycznie aktualizował sygnatury zagrożeń. -System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. -Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, appletów Java czy ciasteczek. -Rozwiązanie musi przeprowadzać emulację skryptów Java. -Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta.

		<ul style="list-style-type: none"> -Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted Applications - PUAs) -System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates) <p>2) Inspekcja ruchu SSL/TLS</p> <ul style="list-style-type: none"> -Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. -Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. -Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. -Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). -Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. -Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen. <p>3) Filtr Web</p> <ul style="list-style-type: none"> -Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron. -Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy. -Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. -System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowania treści komunikatu w tym dodania logo organizacji. -Rozwiązanie powinno umożliwiać filtrowanie stron web analizując ich zawartość wykorzystując tzw. Content Filtering na bazie haseł kluczowych. -Rozwiązanie powinno oferować ochronę przed Pharmingiem.
14.	Ochrona i kontrola aplikacji	<ol style="list-style-type: none"> 1) Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. 2) Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. 3) Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. 4) Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów. 5) Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp. 6) Rozwiązanie powinno oferować funkcje CASB (Cloud Access Security Broker) celem monitorowania i regulowania dostępu do aplikacji chmurowych wykorzystywanych przez użytkowników. 7) Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN.
15.	Licencja i Wsparcie techniczne	Licencja i wsparcie techniczne (gwarancja) producenta na okres minimum 12 miesięcy.

6 Zarządzany przełącznik sieciowy – 2 szt.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Porty dostępne	Przełącznik musi posiadać minimum 48 portów Ethernet 10/100/1000 Mb/s RJ-45 z automatyczną negocjacją prędkości, duplex i Auto-MDI/MDIX.
2.	Porty uplink	Przełącznik musi być wyposażony w minimum 4 porty uplink SFP+ 10Gb/s z obsługą modułów światłowodowych i DAC.
3.	Stacking i skalowalność	Urządzenie musi wspierać hardware stacking do co najmniej 8 przełączników w jednym systemie, z jednolitym zarządzaniem, jednym adresem IP oraz mechanizmem sprzętowego przejęcia roli mastera (failover).
4.	Wydajność i architektura	Urządzenie musi zapewniać non-blocking wire-speed na wszystkich portach oraz wydajność komunikacyjną odpowiednią dla środowisk obsługujących dane, głos i wideo.
5.	Zasilanie PoE i zarządzanie energią	Przełącznik musi obsługiwać PoE/PoE+ zgodne z IEEE 802.3af i 802.3at, z funkcjami: monitorowania zużycia energii per port, sterowania budżetem mocy oraz włączania/wyłączania PoE.
6.	Funkcje warstwy 2	Obsługa VLAN (IEEE 802.1Q), VLAN głosowych, Multicast VLAN (MVR), VLAN protokołowych i MAC-based VLAN, agregacja łączy (LACP), STP/RSTP/MSTP, LLDP/LLDP-MED, IGMP Snooping oraz port mirroring do diagnostyki ruchu.
7.	Funkcje warstwy 3	Przełącznik musi obsługiwać routing statyczny IPv4 i IPv6, DHCP Server i DHCP Relay oraz opcjonalne protokoły dynamicznego routingu zgodne z klasą L3 Lite.
8.	Jakość usług (QoS)	Urządzenie musi zapewniać zaawansowane mechanizmy QoS, m.in. klasyfikację i priorytetyzację ruchu (CoS/DSCP), kolejkovanie WRR, priorytet IPS, rozróżnianie typów ruchu głosowego, wideo i krytycznego biznesowo.
9.	Bezpieczeństwo sieci	Obsługa co najmniej: uwierzytelnianie IEEE 802.1X z dynamicznym VLAN, ACL do 2048/3072 reguł, Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, IPv6 First Hop Security, RADIUS/TACACS+, ochrona przed DoS i mechanizmy związane z ochroną sterowania STP (BPDU Guard, Root Guard)
10.	Widoczność i diagnostyka	Przełącznik musi dostarczać szczegółowe statystyki portów, monitorowanie stanu PoE, pasma, temperatury oraz rejestrowanie zdarzeń i alertów.
11.	Zarządzanie i integracja	Możliwość zarządzania: Dashboard, mobile app oraz interfejs zarządzania WWW i CLI. Obsługa SNMP v1/v2c/v3, syslog, NTP i integracji z narzędziami zewnętrznymi.
12.	Efektywność energetyczna	Urządzenie musi wspierać standard IEEE 802.3az Energy Efficient Ethernet oraz mechanizmy automatycznego wyłączania portów bez aktywnego linku i inteligentne sterowanie energią na
13.	Obudowa i montaż	Urządzenie musi być przystosowane do montażu w standardowej szafie rack 19", o wysokości nie większej niż 1U, z kompletem uchwytów montażowych
14.	Zasilanie	Zasilanie z sieci 230V AC.
15.	Gwarancja	Gwarancja producenta na okres minimum 24 miesięcy.

7 Urządzenie pamięci masowej – typ I – 1 szt.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Typ obudowy	Urządzenie musi być przystosowane do montażu w szafie rack 19", o wysokość maksymalnie 2U z możliwością instalacji minimum 12 dysków 3.5" .
2.	Przestrzeń	Zainstalowane: 3 x 1.92TB SSD SAS, Read Intensive, up to 24Gbps 512e 2.5".

	dyskowa	
3.	Możliwość rozbudowy	Urządzenie musi umożliwiać rozbudowę (bez wymiany kontrolerów pamięci masowej), do co najmniej 264 dysków twardych.
4.	Obsługa dysków	1) Urządzenie musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. 2) Urządzenie musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Urządzenie musi obsługiwać dyski 2,5" jak również 3,5".
5.	Sposób zabezpieczenia danych	1) Urządzenie musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej pamięci masowej i z wykorzystaniem wszystkich dysków (tzw. wide-striping). 2) Urządzenie musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. 3) Urządzenie musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności pamięci masowej, zwiększenie szybkości odbudowy pamięci masowej na wypadek awarii dysku). 4) Urządzenie musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
6.	Tryb pracy kontrolerów macierzowych	1) Urządzenie musi posiadać minimum 2 kontrolery dyskowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. 2) Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
7.	Pamięć cache	1) Urządzenie musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. 2) Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. 3) Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
8.	Rozbudowa pamięci cache	1) Urządzenie musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. 2) Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
9.	Interfejsy	Urządzenie musi posiadać, co najmniej 8 portów 10Gb iSCSI BaseT (4 porty na kontroler)
10.	Zarządzanie	1) Zarządzanie pamięcią masową musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. 2) Zarządzanie pamięcią masową musi odbywać się bezpośrednio na kontrolerach dyskowych z poziomu przeglądarki internetowej.
11.	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	1) Urządzenie musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej pamięci masowej. 2) Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne pamięci masowej (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. 3) Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

12.	Thin Provisioning	<ol style="list-style-type: none"> 1) Urządzenie musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. 2) Urządzenie musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach dyskowych (wymagana obsługa standardu T10 SCSI UNMAP). 3) Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
13.	Tiering	<ol style="list-style-type: none"> 1) Urządzenie musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. 2) Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. 3) Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
14.	Wewnętrzne kopie migawkowe	<ol style="list-style-type: none"> 1) Urządzenie musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach pamięci masowej za pomocą wewnętrznych kontrolerów dyskowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. 2) Urządzenie musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
15.	Wewnętrzne kopie pełne	<ol style="list-style-type: none"> 1) Urządzenie musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach pamięci masowej za pomocą wewnętrznych kontrolerów dyskowych. 2) Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
16.	Migracja danych w obrębie macierzy	<ol style="list-style-type: none"> 1) Urządzenie musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). 2) Zmiany te muszą się odbywać wewnętrznymi mechanizmami pamięci masowej. 3) Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez pamięć masową, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. 4) Zmiany te muszą się odbywać wewnętrznymi mechanizmami pamięci masowej. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
17.	Zdalna replikacja danych	<ol style="list-style-type: none"> 1) Urządzenie musi umożliwiać asynchroniczną replikację danych do innej pamięci masowej z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do pamięci masowej. 2) Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
18.	Podłączanie zewnętrznych systemów	<ol style="list-style-type: none"> 1) Urządzenie musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).

	operacyjnych	<ol style="list-style-type: none">2) Urządzenie musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.3) Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.4) Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
19.	Redundancja	<ol style="list-style-type: none">1) Urządzenie nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.2) Urządzenie musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.3) Urządzenie musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy pamięci masowej.4) Zasilacze użyte w pamięci masowej powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
20.	Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej pamięci masowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu urządzeń pamięci masowej. Za pojedynczą pamięć masową nie uznaje się rozwiązania opartego o wiele pamięciach masowych (par kontrolerów dyskowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem pamięci masowej.
21.	Inne	<ol style="list-style-type: none">1) Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.2) Oferowany model pamięci masowej w momencie składania oferty nie może mieć ogłoszonej daty końca sprzedaży. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające brak ogłoszenia takiej daty.3) Sprzęt musi być wyprodukowany zgodnie z normami ISO 9001 oraz ISO 14001.4) Sprzęt musi posiadać deklarację zgodności CE.
22.	Gwarancja i serwis (Kryterium Punktowe)	<ol style="list-style-type: none">1) Gwarancja producenta: min. 36 miesięcy lub dłużej zgodnie ze złożoną ofertą realizowanej przez producenta lub autoryzowanego partnera serwisowego producenta..2) Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie lub przez Internet.3) <u>Wymagane dołączenie do oferty oświadczenia Wykonawcy lub Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</u>4) W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – <u>wymagane jest dołączenie do oferty oświadczenia podmiotu wykonującego Serwis lub Producenta potwierdzające powyższe.</u>5) Firma serwisująca musi posiadać ISO9001 oraz ISO27001 na świadczenie usług serwisowych oraz posiada autoryzację producenta urządzeń – <u>dokumenty potwierdzające należy załączyć do oferty.</u>

8 Urządzenie pamięci masowej – typ II – 1 szt.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Charakterystyka ogólna urządzenia	<p>6) Pamięć masowa musi być urządzeniem sieciowym przeznaczonym do pracy ciągłej 24/7, wyposażonym w redundantne zasilanie, umożliwiającym montaż w standardowej szafie teleinformatycznej RACK 19" (wysokość maksymalnie 1U).</p> <p>7) Rozwiązanie musi integrować w jednej platformie funkcje:</p> <ul style="list-style-type: none"> - centralnego repozytorium danych, - serwera plików dla wielu systemów operacyjnych, - platformy kopii zapasowych i replikacji danych, - środowiska wirtualizacji i konteneryzacji.
2.	System operacyjny i zarządzanie	<p>1) Pamięć masowa musi być wyposażona w dedykowany system operacyjny producenta, umożliwiający zarządzanie urządzeniem poprzez interfejs graficzny dostępny z poziomu przeglądarki internetowej.</p> <p>2) System musi zapewniać:</p> <ul style="list-style-type: none"> - centralne zarządzanie przestrzenią dyskową i wolumenami, - tworzenie i zarządzanie przestrzeniami RAID, - monitorowanie stanu sprzętu i zasobów, - rozbudowany system powiadomień i alertów, - wielopoziomowy system uprawnień użytkowników i grup.
3.	Bezpieczeństwo danych	<p>Rozwiązanie musi oferować zaawansowane mechanizmy ochrony danych, w tym:</p> <ol style="list-style-type: none"> 1) obsługę migawek (snapshots) wolumenów i udziałów, 2) możliwość szybkiego przywracania danych po awarii lub ataku ransomware, 3) szyfrowanie danych przechowywanych na dyskach, 4) integrację z usługami katalogowymi (Active Directory / LDAP), 5) wbudowaną zaporę sieciową oraz mechanizmy ochrony przed złośliwym oprogramowaniem.
4.	Kopie zapasowe i replikacja	<p>1) Pamięć masowa musi umożliwiać realizację kopii zapasowych:</p> <ul style="list-style-type: none"> - danych lokalnych, - danych z innych serwerów i stacji roboczych, - maszyn wirtualnych, - danych do lokalizacji zdalnych oraz chmury obliczeniowej. <p>2) System musi obsługiwać replikację danych w trybie asynchronicznym oraz synchronizację między lokalizacjami.</p>
5.	Wirtualizacja i konteneryzacja	<p>Urządzenie musi umożliwiać:</p> <ol style="list-style-type: none"> 1) uruchamianie maszyn wirtualnych, 2) obsługę kontenerów Docker i LXC, 3) integrację z zewnętrznymi środowiskami wirtualnymi jako magazyn danych.
6.	Architektura sprzętowa i programowa pamięci masowej	<ol style="list-style-type: none"> 1) Platforma sprzętowa oparta o architekturę x86-64. 2) Procesor czterordzeniowy, klasy serwerowej, obsługujący sprzętową wirtualizację oraz instrukcje kryptograficzne. 3) Pamięć RAM: minimum 8 GB, z możliwością rozbudowy do co najmniej 16 GB. 4) Wbudowana pamięć flash do przechowywania systemu operacyjnego.

		<p>5) Zatoki dyskowe: minimum 4 zatoki obsługujące dyski 3,5" HDD oraz 2,5" SSD.</p> <p>6) Interfejs dysków: SATA III 6 Gb/s z obsługą dysków klasy enterprise.</p> <p>7) Sprzętowa lub programowa obsługa RAID: RAID 0, 1, 5, 6, 10 oraz JBOD.</p> <p>8) Porty Ethernet 2.5GbE: minimum 2 porty, z możliwością agregacji łączy.</p> <p>9) Protokoły sieciowe: obsługa SMB/CIFS, NFS, FTP, SFTP, iSCSI, WebDAV.</p> <p>10) Porty USB 3.x: minimum 2 porty do podłączania nośników zewnętrznych oraz urządzeń peryferyjnych, np. UPS.</p> <p>11) zainstalowane cztery dyski twarde typu HDD o pojemności nie mniejszej niż 8 TB każdy, z interfejsem SATA III, w formacie 3,5", o prędkości obrotowej min. 7 200 RPM, wyposażone w pamięć podręczną o pojemności co najmniej 256 MB, o współczynniku obciążenia rocznego do 550 TB oraz deklarowanym MTBF nie mniejszym niż 2,3 mln godzin.</p>
7.	Gwarancja i serwis (Kryterium Punktowe)	<p>1) Gwarancja producenta: min. 36 miesięcy lub dłużej zgodnie ze złożoną ofertą realizowanej przez producenta lub autoryzowanego partnera serwisowego producenta.</p> <p>2) W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – <u>wymagane jest dołączenie do oferty oświadczenia podmiotu wykonującego Serwis lub Producenta potwierdzające powyższe.</u></p>

9 UPS – 2 szt.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Przeznaczenie i zastosowanie	<p>1) Zasilacz UPS przeznaczony do zabezpieczenia ciągłości zasilania krytycznych systemów informatycznych i telekomunikacyjnych, w tym:</p> <ul style="list-style-type: none"> - serwery i systemy storage, - urządzenia VoIP i sieciowe, - urządzenia przemysłowe.
2.	Zakres funkcjonalny	<p>1) Urządzenie musi zapewniać:</p> <ul style="list-style-type: none"> - podtrzymanie zasilania i filtrowanie napięcia w trakcie zaniku sieci, - ochronę przed przepięciami, zakłóceniami i odkształceniami napięcia, - automatyczne przełączanie na zasilanie bateryjne bez przerwy w dostawie energii.
3.	Podstawowe parametry techniczne	<p>1) Moc i wejście</p> <ul style="list-style-type: none"> - Moc pozorna: min. 3000 VA - Moc czynna: min. 2700 W - Napięcie wejściowe: 220–240 V AC - Częstotliwość pracy: 50/60 Hz ±5% <p>2) Wyjście i jakość zasilania</p> <ul style="list-style-type: none"> - Typ zasilania: ON LINE – podwójna konwersja - Częstotliwość wyjściowa: wybieralna (50 Hz / 60 Hz / auto) - Przebieg napięcia: sinusoidalny - Współczynnik mocy wyjściowej: >0,98 - Obciążalność wyjścia: do 150% mocy znamionowej przez ograniczony czas <p>3) Baterie</p>

		- Typ: bezobsługowe - Czas ładowania typowy: max. 2–4 h
4.	Komunikacja i interfejsy sterujące	1) Urządzenie musi posiadać: - port USB do integracji z systemami monitoringu, - port RS232 (DB9) z izolacją galwaniczną, - slot komunikacyjny umożliwiający instalację kart SNMP / Modbus / TCP-IP, - oprogramowanie nadzorcze i do automatycznego zamykania systemów.
5.	Tryby pracy	1) podstawowy tryb podwójnej konwersji, 2) ekonomiczny tryb wysokiej efektywności (↑98%), 3) automatyczne przełączanie trybów zależne od jakości sieci, 4) tylko podtrzymanie przy zaniku sieci, 5) Funkcja konwersji częstotliwości – 50/60 Hz
6.	Wymagania środowiskowe	1) Temperaturowy zakres pracy: min. 0–40 °C 2) Wilgotność pracy: min. 5–95% bez kondensacji 3) Poziom hałasu: <40 dBA
7.	Wymiary i montaż	1) Format: max. 2U do szafy 19” 2) Wymiary maksymalnie (WxDxH): 90×450×650 mm 3) Masa maksymalnie: 32 kg
8.	Normy i certyfikaty	Oferowany zasilacz UPS musi posiadać oznaczenie CE oraz być zgodny z dyrektywami 2014/35/EU (LVD) i 2014/30/EU (EMC), a także spełniać wymagania norm EN 62040-1 oraz EN 62040-2.
9.	Gwarancja	Gwarancja producenta na okres minimum 24 miesięcy.

10 Sprzętowy klucz bezpieczeństwa – 20 szt.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Interfejsy	USB-A (podłączany bezpośrednio do komputera)
2.	NFC	TAK (komunikacja bezprzewodowa z urządzeniami mobilnymi zgodnymi z NFC)
3.	Obsługiwane protokoły bezpieczeństwa	FIDO2 U2F (Universal 2nd Factor) Smart Card OpenPGP OATH-TOTP (jednorazowe hasła czasowe) OATH-HOTP (jednorazowe hasła zdarzeniowe) Challenge-Response
4.	Zgodność systemowa	Windows, macOS, Linux iOS, Android (przez NFC lub odpowiedni adapter USB)
5.	Budowa i trwałość	Wykonanie odporne na wodę i wstrząsy Brak wbudowanej baterii i połączenia sieciowego (wysoki poziom bezpieczeństwa fizycznego)
6.	Bezpieczeństwo	Klucze prywatne generowane i przechowywane wyłącznie na urządzeniu (nie opuszczają klucza)

		Certyfikaty: zgodność FIPS, NIST
7.	Gwarancja	Minimum 24 miesięcy

11 Oprogramowanie typu CMDB i SAM – 1 kpl.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Wymagania ogólne dla systemu	<ol style="list-style-type: none"> Oprogramowanie musi posiadać polski oraz angielski interfejs językowy. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta/Konsoli zarządzającej. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwerem aplikacji i konsolą zarządzającą. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników. Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym, tj. bez wkompiowanych funkcji takich jak zdalne zarządzanie, transfer plików czy zdalny pulpit. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji operatorów konsoli zarządzającej z wykorzystaniem fizycznego zabezpieczenia sprzętowego (lokalnego lub sieciowego) wraz z hasłem, umożliwiającą jednoczesną pracę wielu administratorów. Logowanie musi umożliwiać integrację z Active Directory, a zabezpieczenie sprzętowe musi wykorzystywać szyfrowanie AES. Oprogramowanie musi obsługiwać dodatkową autoryzację użytkowników konsoli za pomocą Google Authenticator oraz Microsoft Authenticator. Oprogramowanie musi posiadać mechanizm zarządzania uprawnieniami zgodny z modelem RBAC (Role Based Access Control) Oprogramowanie musi współpracować z bazą danych Microsoft SQL Server w wersjach 2008R2–2019. Oprogramowanie nie może wymagać komponentów Java do prawidłowej pracy. Oprogramowanie serwera aplikacji musi posiadać funkcję centralnego wysyłania powiadomień e-mail. Oprogramowanie musi posiadać mechanizm zarządzania uprawnieniami do danych w kontekście jednostek organizacyjnych i typów zasobów. Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem z poprawną ścieżką certyfikacji w systemie Windows. Oprogramowanie agentów musi obsługiwać sesje terminalowe Windows. Oprogramowanie musi zapewniać dziedziczenie konfiguracji agentów oraz natychmiastowe (online) stosowanie zmian.
2.	Inwentaryzacja konfiguracji komputerów	<ol style="list-style-type: none"> Oprogramowanie musi umożliwiać druk kartotek sprzętowych oraz ich graficzną edycję. Oprogramowanie musi umożliwiać projektowanie i druk etykiet inwentaryzacyjnych z kodami kreskowymi EAN128 oraz PDF417. Oprogramowanie musi realizować okresową automatyczną inwentaryzację parametrów sprzętowych, takich jak HDD, RAM, CPU, karta sieciowa, karta graficzna oraz system operacyjny.

		<p>4) Oprogramowanie musi umożliwiać analizę sprzętu, systemu operacyjnego, informacji sieciowych oraz historii zmian sprzętowych.</p> <p>5) Oprogramowanie musi umożliwiać monitorowanie obciążenia CPU i RAM z zapisem historii</p>
3.	Inwentaryzacja oprogramowania	<p>1) Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego oprogramowania.</p> <p>2) Oprogramowanie musi umożliwiać tworzenie zestawień programów, systemów operacyjnych oraz wykazów brakujących aplikacji.</p> <p>3) Oprogramowanie musi umożliwiać zdalną dezinstalację oprogramowania oraz blokowanie procesów.</p> <p>4) Oprogramowanie musi umożliwiać klasyfikację aplikacji jako zgodnych lub zabronionych oraz raportowanie.</p> <p>5) Oprogramowanie musi umożliwiać zdalne usuwanie nielegalnych danych.</p>
4.	Zarządzanie licencjami i audyt oprogramowania	<p>1) Oprogramowanie musi posiadać bazę sygnatur aplikacji z automatyczną aktualizacją.</p> <p>2) Oprogramowanie musi umożliwiać definiowanie własnych sygnatur oraz audyt licencji z obsługą downgrade i upgrade.</p> <p>3) Oprogramowanie musi umożliwiać prowadzenie bazy licencji i przypisywanie ich do użytkowników oraz stanowisk.</p>
5.	CMDB	<p>1) Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI).</p> <p>2) Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI, w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe. Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI. Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny.</p> <p>3) Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI.</p> <p>4) Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji. Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej.</p> <p>5) Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji.</p> <p>6) Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami.</p> <p>7) Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji.</p> <p>8) Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV).</p> <p>9) Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji.</p> <p>10) Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji według posiadanych atrybutów.</p> <p>11) Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowej i odwrotnej.</p> <p>12) Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji.</p>

6.	Zarządzanie zasobami i użytkownikami	<ol style="list-style-type: none"> 1) Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami. 2) Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu. 3) Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość. 4) Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów. 5) Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiązania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem. 6) Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych. 7) Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów. 8) Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu. 9) Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV. 10) Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej. 11) Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu. 12) Oprogramowanie musi umożliwiać eksport ww. protokołów w formacie PDF. 13) Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków. 14) Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji. 15) Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu. 16) Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu. 17) Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu. 18) Oprogramowanie musi umożliwiać podgląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu. 19) Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego. 20) Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu. 21) Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami. 22) Oprogramowanie musi umożliwiać seryjne dodawanie zasobów.
----	--------------------------------------	--

		<p>23) Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów.</p> <p>24) Oprogramowanie musi udostępniać kreator raportów dla zasobów.</p> <p>25) Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typu zasobu.</p> <p>26) Oprogramowanie musi udostępniać możliwość kopiowania formularza dla określonego typu(ów) zasobu z innego typu zasobu.</p> <p>27) Oprogramowanie musi umożliwiać ewidencję magazynów.</p> <p>28) Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych.</p> <p>29) Oprogramowanie musi umożliwiać ewidencję produktów magazynowych.</p> <p>30) Oprogramowanie musi udostępniać informację o stanie magazynowym (ilościowo).</p> <p>31) Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM.</p> <p>32) Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn.</p>
7.	Zdalny pulpit, zdalne zarządzanie komputerem	<p>1) Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpitu nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).</p> <p>2) Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.</p> <p>3) Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie: tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta.</p> <p>4) Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.</p> <p>5) Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.</p> <p>6) Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).</p> <p>7) Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.</p> <p>8) Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.</p> <p>9) Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.</p> <p>10) Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.</p>
8.	Automatyzacja	<p>1) Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.</p>

		<ol style="list-style-type: none"> 2) Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych. 3) Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych. 4) Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk. 5) Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności. 6) Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji. 7) Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr). 8) Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle). 9) Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD. 10) Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji. 11) Oprogramowanie musi umożliwiać instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.) 12) Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji. 13) Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika. 14) Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera).
9.	Zarządzanie urządzeniami USB Storage	<ol style="list-style-type: none"> 1) Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny. 2) Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane. 3) Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage. 4) Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage. 5) Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD.

10.	Monitoring stanowisk komputerowych	<ol style="list-style-type: none"> 1) Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony. 2) Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik. 3) Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk). 4) Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach. 5) Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego). 6) Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk. 7) Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione. 8) Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności). 9) Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer. 10) Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania.
11.	ServiceDesk – Zarządzanie zgłoszeniami	<ol style="list-style-type: none"> 1) Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności: <ul style="list-style-type: none"> - Zarządzanie problemem; - Zarządzanie incydem; - Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy); - Zarządzanie umowami serwisowymi; - Definicje poziomów SLA (reakcja, naprawa, reklamacja). 2) Oprogramowanie musi umożliwiać zgłaszanie przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora. 3) Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika. 4) Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu. 5) Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP. 6) Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmu SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń. 7) Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu. 8) Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia. 9) Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.

		<p>10) Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.</p> <p>11) Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.</p> <p>12) Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.</p> <p>13) Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:</p> <ul style="list-style-type: none"> - Zmiana statusu po przejściu zgłoszenia przez opiekuna. - Przejmowanie zadań po przejściu zgłoszenia przez opiekuna. - Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia. - Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika. - Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika. - Zamykanie zgłoszenia po upływie czasu reklamacji. - Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów. - Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza. - Walidacja zamkniętych zadań w zamykanym zg
12.	ServiceDesk – Zarządzanie wnioskami	<p>1) Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).</p> <p>2) Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.</p> <p>3) Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.</p>
13.	ServiceDesk – Zarządzanie uprawnieniami	<p>1) Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych.</p> <p>2) Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych.</p> <p>3) Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych).</p> <p>4) Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych.</p> <p>5) Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem Informatycznym lub Zbiorem danych po akceptacji wniosku.</p> <p>6) Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika).</p> <p>7) Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób.</p> <p>8) Oprogramowanie musi umożliwiać raportowanie uprawnień pracowników do Systemów Informatycznych oraz Zbiorów danych.</p> <p>9) Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika.</p>

14.	ServiceDesk – Zarządzanie rezerwacjami	<ol style="list-style-type: none"> 1) Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie. 2) Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji. 3) Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika. 4) Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia lub edycji rezerwacji z zasobem. 5) Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza. 6) Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.
15.	Monitoring sieci LAN	<ol style="list-style-type: none"> 1) Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej: komputery, drukarki, routery, smartfony. 2) Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek, tj. poziomy tonerów, liczba wydrukowanych stron oraz informowanie o błędach takich jak brak papieru lub zacięcie papieru. 3) Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch lub router. 4) Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP (v1/v2/v3) urządzenia. 5) Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytanie typu PING. 6) Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub e-mail.
16.	Zarządzanie dokumentami	<ol style="list-style-type: none"> 1) Oprogramowanie musi umożliwiać centralną ewidencję dokumentów. 2) Oprogramowanie musi umożliwiać posiadanie dedykowanego formularza dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu. 3) Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in. skany faktur, umów). 4) Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów. 5) Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników. 6) Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym. 7) Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących.
17.	System zarządzania urządzeniami mobilnymi	<ol style="list-style-type: none"> 1) Oprogramowanie musi umożliwiać centralne zarządzanie urządzeniami mobilnymi. 2) Oprogramowanie musi umożliwiać zdalne przywracanie systemu do ustawień fabrycznych. 3) Oprogramowanie musi umożliwiać wykonanie zrzutu ekranu urządzenia (screen). 4) Oprogramowanie musi umożliwiać pobranie logów urządzenia. 5) Oprogramowanie musi umożliwiać skanowanie plików urządzenia.

		<ol style="list-style-type: none"> 6) Oprogramowanie musi umożliwiać zarządzanie politykami bezpieczeństwa np. hasłami. 7) Oprogramowanie musi umożliwiać backup kontaktów, połączeń, SMS-ów, rejestru połączeń. 8) Oprogramowanie musi umożliwiać automatyczne pozyskiwanie informacji w zakresie m.in. nazwa, model, wersja systemu, model urządzenia, rodzaj procesora, ilość pamięci RAM, pamięć na karcie SD, karta SIM, numer telefonu, numer IMEI, numer seryjny, ostatnia aktywność agenta. 9) Oprogramowanie musi udostępniać pełen log z działania urządzenia (np. zarządzanie łącznością, ponowne uruchomienie urządzenia). 10) Oprogramowanie musi umożliwiać dostęp do mapy z aktualną lokalizacją urządzenia. 11) Oprogramowanie musi umożliwiać inwentaryzację zainstalowanych aplikacji na urządzeniu. 12) Oprogramowanie musi umożliwiać inwentaryzację plików znajdujących się na urządzeniu. 13) Oprogramowanie musi umożliwiać podgląd listy historycznie wykonanych zadań. 14) Oprogramowanie musi posiadać wbudowane raporty dotyczące urządzeń mobilnych w zakresie minimalnym: według producenta, wersji, ostatniej aktywności, systemu operacyjnego. 15) Oprogramowanie musi umożliwiać wysyłanie wiadomości na urządzenie. 16) Oprogramowanie musi umożliwiać połączenie zdalne z urządzeniem. 17) Oprogramowanie musi umożliwiać zarządzanie urządzeniem w oparciu o polityki w zakresie: łączność, aplikacje, ogólne zarządzanie, hasła. 18) Oprogramowanie musi umożliwiać zarządzanie urządzeniem w oparciu o profile w zakresie: WiFi, lokalizacja, KIOSK, kontakty. 19) Oprogramowanie musi umożliwiać zarządzanie urządzeniem w oparciu o reguły (np. przypisywanie polityk i profili). 20) Oprogramowanie musi umożliwiać odtworzenie backupu SMS-ów, kontaktów oraz rejestru połączeń. 21) Oprogramowanie musi umożliwiać podgląd listy wszystkich wykonanych backupów urządzenia.
18.	Wymagania formalne	<ol style="list-style-type: none"> 1) Dostarczone licencje na oprogramowanie muszą być bezterminowe. 2) Dostarczone licencje muszą obejmować 12-miesięczny support producenta liczony od daty zakończenia wdrożenia. 3) Obsługa serwisowa musi być realizowana z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych, z dostępem do nowych wersji systemu i wsparcia technicznego producenta. 4) Licencje muszą obejmować co najmniej 38 stanowisk komputerowych z systemem Microsoft Windows oraz 38 urządzeń mobilnych z systemem Android, bez limitu na inne zasoby oraz z co najmniej jedną licencją dostępową do konsoli zarządzającej. 5) Zamawiający zastrzega sobie prawo do wezwania wykonawcy do prezentacji rozwiązania w terminie do 7 dni od otwarcia ofert. 6) Producent oprogramowania musi posiadać certyfikat potwierdzający zgodność z normą ISO 27001. 7) Zamawiający wymaga posiadania aktualnego certyfikatu zgodności z najlepszymi praktykami ITSM w zakresie Incident Management, Problem Management, Knowledge Management oraz Asset Management, wydanego przez niezależną organizację

		certyfikującą – <u>Do oferty należy dołączyć kopię certyfikatu oraz link do strony organizacji certyfikującej.</u>
--	--	--

12 Oprogramowanie klasy EDR – 1 kpl.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Ogólne	<p>1) Komplet oprogramowania musi zapewniać funkcjonalności klasy Endpoint Detection and Response (EDR/EPP) oraz obejmować mechanizmy ochrony danych na stacjach końcowych, wspierające zapobieganie nieautoryzowanemu wynoszeniu, kopiowaniu lub przesyłaniu danych.</p> <p>2) Rozwiązanie musi umożliwiać centralne zarządzanie konsolowe z wykorzystaniem przeglądarki WWW, zgodnie z architekturą oferowanego rozwiązania.</p>
2.	Ochrona endpointów	Rozwiązanie musi zapewniać zaawansowaną ochronę endpointów obejmującą wykrywanie znanych i nieznanych zagrożeń z wykorzystaniem mechanizmów sztucznej inteligencji i deep learning, ochronę behawioralną opartą na analizie zachowania procesów, plików i rejestru, ochronę przed exploitami pamięci i aplikacji, ochronę przed ransomware lokalnym i zdalnym wraz z możliwością automatycznego przywracania plików po ataku oraz zabezpieczenie sektora rozruchowego dysku (MBR).
3.	Redukcja powierzchni ataku	Oprogramowanie musi umożliwiać kontrolę dostępu do stron internetowych, aplikacji, urządzeń peryferyjnych oraz nośników danych, a także egzekwowanie polityk bezpieczeństwa na poziomie endpointów.
4.	EDR	Rozwiązanie musi zapewniać funkcje Endpoint Detection and Response, w tym zbieranie danych telemetrycznych, korelację zdarzeń bezpieczeństwa, automatyczną ocenę ryzyka incydentów oraz przechowywanie danych telemetrycznych przez minimum 30 dni.
5.	Reakcja na incydenty	Oprogramowanie musi umożliwiać reakcję na incydenty bezpieczeństwa, w tym izolację sieciową endpointów, zatrzymywanie procesów, cofanie skutków ataków oraz zdalny dostęp administracyjny do chronionych systemów.
6.	Zarządzanie	Rozwiązanie musi zapewniać centralne zarządzanie politykami bezpieczeństwa, predefiniowane ustawienia ochrony, pulpity administracyjne oraz możliwość generowania raportów.
7.	Ochrona informacji	Rozwiązanie musi umożliwiać klasyfikację informacji przetwarzanych na stacjach roboczych i w zasobach sieciowych w oparciu o zawartość plików, ich format, lokalizację oraz aplikację źródłową.
8.	Egzekwowanie reguł offline	Reguły bezpieczeństwa dotyczące przetwarzania informacji muszą być egzekwowane również w przypadku braku połączenia endpointa z centralną konsolą, z lokalnym buforowaniem zdarzeń do czasu synchronizacji.
9.	Kontrola operacji na danych	Dla informacji zaklasyfikowanych jako wrażliwe system musi umożliwiać definiowanie reguł zezwalających lub blokujących operacje takie jak kopiowanie, przenoszenie, drukowanie, zapisywanie oraz przesyłanie do usług chmurowych lub pocztowych.
10.	Analiza treści	Weryfikacja zawartości plików musi odbywać się w czasie rzeczywistym, w tym z wykorzystaniem mechanizmów rozpoznawania treści w dokumentach graficznych i zeskanowanych.
11.	Audyt i integracje	System musi umożliwiać szczegółowy audyt operacji użytkowników na danych oraz eksport zdarzeń do zewnętrznych systemów analitycznych klasy SIEM.
12.	Integracja katalogowa	Rozwiązanie musi umożliwiać synchronizację użytkowników i grup z usługą katalogową Active Directory w celu przypisywania polityk bezpieczeństwa.

13.	Obsługiwane systemy operacyjne	Microsoft Windows i Microsoft Windows Server (aktualnie wspierane wersje).
14.	Okres utrzymania funkcjonalności.	Oprogramowanie musi posiadać zapewnione aktualizacje bezpieczeństwa i funkcjonalne przez okres minimum 12 miesięcy.

13 Oprogramowanie do archiwizacji – 1 kpl.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Przeznaczenie	Oprogramowanie do tworzenia, zarządzania oraz odtwarzania kopii zapasowych danych, przeznaczone do ochrony danych systemów informatycznych poprzez wykonywanie kopii zapasowych oraz zapewnienie szybkiego i skutecznego odtwarzania danych w przypadku awarii, błędu użytkownika lub ataku cybernetycznego.
2.	Architektura rozwiązania	Oprogramowanie w postaci aplikacji serwerowej z centralnym panelem zarządzania oraz opcjonalnymi agentami instalowanymi na chronionych systemach.
3.	Obsługiwane środowiska	Oprogramowanie musi obsługiwać co najmniej: <ul style="list-style-type: none"> - systemy fizyczne (stacje robocze i serwery), - środowiska wirtualne, - usługi chmurowe typu SaaS.
4.	Zakres funkcjonalny backupu	Oprogramowanie musi umożliwiać: <ul style="list-style-type: none"> - pełne, przyrostowe i różnicowe kopie zapasowe, - harmonogramowanie zadań backupu, - przechowywanie wielu wersji danych.
5.	Odzyskiwanie danych	Oprogramowanie musi umożliwiać: <ul style="list-style-type: none"> - odtwarzanie pojedynczych plików, - odtwarzanie całych systemów lub maszyn wirtualnych, - przywracanie danych do lokalizacji pierwotnej lub alternatywnej.
6.	Optymalizacja przestrzeni	Oprogramowanie musi oferować mechanizmy ograniczające zajętość danych kopii zapasowych, takie jak: <ul style="list-style-type: none"> - deduplikacja, - kompresja danych.
7.	Bezpieczeństwo danych	Oprogramowanie musi zapewniać szyfrowanie danych w trakcie transmisji.
8.	Zarządzanie i administracja	Oprogramowanie musi posiadać centralny interfejs administracyjny umożliwiający konfigurację, nadzór oraz zarządzanie wszystkimi zadaniami backupu.
9.	Monitorowanie i raportowanie	Oprogramowanie musi zapewniać: <ul style="list-style-type: none"> - monitorowanie statusu zadań backupu, - raportowanie sukcesów i błędów.
10.	Skalowalność	Oprogramowanie musi umożliwiać rozbudowę zakresu ochrony danych (np. zwiększenie liczby chronionych systemów lub wolumenu danych) bez konieczności wymiany całego rozwiązania.
11.	Licencja	Oprogramowanie musi być dostarczone z legalną licencją umożliwiającą jego użytkowanie zgodnie z przeznaczeniem przez okres minimum 12 miesięcy.
12.	Aktualizacje	W okresie obowiązywania licencji Zamawiający musi mieć dostęp do aktualizacji oprogramowania i poprawek bezpieczeństwa.
13.	Dokumentacja	Oprogramowanie musi posiadać dokumentację użytkownika i administratora w języku

		polskim lub angielskim.
--	--	-------------------------

14 Oprogramowanie do wirtualizacji – 1 kpl.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Informacje ogólne	<ol style="list-style-type: none"> 1) Przedmiotem zamówienia jest dostarczenie, wdrożenie oraz konfiguracja platformy wirtualizacji serwerowej przeznaczonej do pracy w środowisku produkcyjnym Zamawiającego. 2) Platforma wirtualizacji musi umożliwiać konsolidację zasobów sprzętowych oraz uruchamianie wielu niezależnych maszyn wirtualnych i kontenerów systemowych na wspólnej infrastrukturze fizycznej. 3) Rozwiązanie musi być oparte o architekturę klastrową i zapewniać centralne zarządzanie środowiskiem składającym się z minimum trzech hostów fizycznych. 4) Platforma musi być rozwiązaniem stabilnym, rozwijanym i wspieranym przez producenta, posiadającym udokumentowane zastosowania w środowiskach produkcyjnych. 5) System musi umożliwiać dalszą rozbudowę środowiska o kolejne hosty bez konieczności przerywania pracy istniejących usług.
2.	Architektura sprzętowa i programowa	<ol style="list-style-type: none"> 1) Platforma wirtualizacji musi być instalowana bezpośrednio na sprzęcie fizycznym typu bare-metal, bez konieczności stosowania dodatkowego systemu operacyjnego jako warstwy pośredniczącej. 2) System musi być dostarczony oraz wdrożony w najnowszej stabilnej wersji produkcyjnej, dostępnej u producenta na dzień publikacji ogłoszenia o zamówieniu. 3) Rozwiązanie musi wykorzystywać sprzętowe mechanizmy wirtualizacji procesora oraz pamięci dostępne w architekturze x86-64. 4) System musi umożliwiać jednoczesne uruchamianie maszyn wirtualnych opartych o różne systemy operacyjne, w tym systemy z rodziny Linux oraz Microsoft Windows. 5) Platforma musi obsługiwać zarówno pełną wirtualizację maszyn wirtualnych, jak i wirtualizację na poziomie systemu operacyjnego w postaci kontenerów systemowych. 6) Rozwiązanie musi zapewniać centralny interfejs administracyjny umożliwiający zarządzanie hostami, maszynami wirtualnymi oraz kontenerami z jednego miejsca.
3.	Klaster i wysoka dostępność	<ol style="list-style-type: none"> 1) Platforma musi umożliwiać tworzenie i zarządzanie klastrem wirtualizacyjnym składającym się z co najmniej trzech hostów fizycznych. 2) System musi zapewniać synchronizację konfiguracji pomiędzy hostami wchodzącymi w skład klastra. 3) Platforma musi posiadać wbudowane mechanizmy wysokiej dostępności umożliwiające automatyczne reagowanie na awarie hostów fizycznych. 4) W przypadku awarii jednego z hostów system musi umożliwiać automatyczne uruchomienie maszyn wirtualnych na pozostałych hostach klastra. 5) Platforma musi umożliwiać definiowanie polityk wysokiej dostępności, w tym określanie priorytetów uruchamiania maszyn wirtualnych.
4.	Migracja i ciągłość pracy	<ol style="list-style-type: none"> 1) System musi umożliwiać migrację maszyn wirtualnych pomiędzy hostami klastra bez przerywania ich pracy. 2) Platforma musi umożliwiać planowaną migrację maszyn wirtualnych w celu optymalizacji wykorzystania zasobów sprzętowych. 3) Rozwiązanie musi umożliwiać przenoszenie maszyn wirtualnych pomiędzy węzłami klastra w celu optymalizacji wykorzystania zasobów.

5.	Pamięć masowa	<ol style="list-style-type: none"> 1) Platforma musi umożliwiać integrację z zewnętrzną, współdzieloną pamięcią masową dostępną jednocześnie dla wszystkich hostów klastra. 2) System musi obsługiwać współdzieloną pamięć masową udostępnianą w oparciu o standardowe protokoły sieciowe, w tym co najmniej NFS oraz iSCSI. 3) Platforma musi umożliwiać przechowywanie dysków maszyn wirtualnych na współdzielonej pamięci masowej. 4) System musi umożliwiać logiczne wydzielanie oraz zarządzanie przestrzenią dyskową przeznaczoną dla maszyn wirtualnych i kontenerów. 5) Platforma musi umożliwiać jednoczesne wykorzystanie lokalnej pamięci masowej hostów oraz współdzielonej pamięci masowej.
6.	Sieć i bezpieczeństwo	<ol style="list-style-type: none"> 1) System musi umożliwiać tworzenie wirtualnych sieci dla maszyn wirtualnych i kontenerów. 2) Platforma musi obsługiwać sieci VLAN w celu logicznej separacji ruchu sieciowego. 3) Rozwiązanie musi umożliwiać agregację interfejsów sieciowych w celu zapewnienia redundancji oraz zwiększenia przepustowości. 4) Platforma musi umożliwiać separację ruchu zarządzającego, migracyjnego oraz ruchu do pamięci masowej. 5) System musi posiadać wbudowany mechanizm zapory sieciowej. 6) Platforma musi umożliwiać definiowanie reguł bezpieczeństwa na poziomie hosta, maszyny wirtualnej oraz kontenera. 7) Rozwiązanie musi wspierać zarządzanie użytkownikami i uprawnieniami w oparciu o role. 8) System musi umożliwiać integrację z zewnętrznymi systemami uwierzytelniania, w tym katalogami LDAP oraz Active Directory.
7.	Kopie zapasowe i odtwarzanie danych	<ol style="list-style-type: none"> 1) Platforma musi posiadać wbudowany mechanizm wykonywania kopii zapasowych maszyn wirtualnych oraz kontenerów. 2) System musi umożliwiać wykonywanie kopii zapasowych w trybie online, bez konieczności wyłączania maszyn wirtualnych. 3) Platforma musi umożliwiać harmonogramowanie kopii zapasowych oraz przechowywanie ich na zewnętrznej pamięci masowej. 4) System musi umożliwiać szybkie i selektywne odtwarzanie maszyn wirtualnych oraz ich zasobów z kopii zapasowych.
8.	Zarządzanie i monitorowanie	<ol style="list-style-type: none"> 1) Platforma musi zapewniać monitorowanie wykorzystania zasobów procesora, pamięci RAM, przestrzeni dyskowej oraz sieci. 2) System musi umożliwiać dostęp do konsoli maszyn wirtualnych bezpośrednio z poziomu interfejsu administracyjnego. 3) Platforma musi udostępniać interfejs programistyczny API umożliwiający integrację z zewnętrznymi systemami zarządzania i automatyzacji. 4) System musi umożliwiać realizację operacji administracyjnych zarówno z poziomu interfejsu graficznego, jak i wiersza poleceń.
9.	Licencjonowanie i wsparcie producenta	<ol style="list-style-type: none"> 1) System musi być objęty licencją lub subskrypcją producenta uprawniającą do legalnego użytkowania rozwiązania w środowisku produkcyjnym. 2) Licencja lub subskrypcja musi być udzielona na okres co najmniej 12 miesięcy od daty odbioru końcowego przedmiotu zamówienia. 3) Licencja lub subskrypcja musi uprawniać Zamawiającego do korzystania z aktualizacji systemu, w tym poprawek bezpieczeństwa, poprawek błędów oraz nowych wersji stabilnych, udostępnianych przez producenta w okresie jej obowiązywania.

		<p>4) System musi być objęty wsparciem technicznym producenta lub autoryzowanego partnera producenta przez cały okres obowiązywania licencji lub subskrypcji.</p> <p>5) Wsparcie techniczne musi obejmować co najmniej dostęp do dokumentacji producenta oraz oficjalnych repozytoriów aktualizacji oprogramowania.</p> <p>6) Po zakończeniu okresu licencji lub subskrypcji Zamawiający musi zachować możliwość dalszego użytkowania systemu zgodnie z warunkami producenta.</p>
--	--	---

15 Instalacja, migracja, wdrożenie – 1 kpl.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Wymagania podstawowe	<p>1) Zamawiający wymaga zrealizowania kompleksowej dostawy, montażu i wdrożenia rozwiązania przy uwzględnieniu kompleksowego działania całości środowiska informatycznego.</p> <p>2) Zamawiający wymaga wyznaczenia osoby w postaci Kierownika Projektu po stronie Wykonawcy jako pojedynczego punktu kontaktowego w zakresie:</p> <ul style="list-style-type: none"> • Uzgodnienia harmonogramu prowadzonych prac, • Koordynowania i uzgadniania terminów dostaw, • Nadzorowania procesu i kompletności realizowania usług związanych z wdrożeniem, • Sporządzania protokołów dostaw i realizacji częściowej/całościowej zakresu wdrożenia. <p>3) Zamawiający, w oparciu o własną wiedzę i doświadczenie, wyspecyfikował niezbędne elementy połączeniowe (wkładki, okablowanie), natomiast w przypadku gdy zajdzie taka potrzeba, wraz z dostarczoną Infrastrukturą, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie dot. redundancji łącz, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie całego Systemu. Dostarczona Infrastruktura musi zapewniać bezproblemową pracę po podłączeniu jej do infrastruktury Zamawiającego.</p>
2.	Wdrożenie rozwiązań – prace montażowo-konfiguracyjne	<p>1) Montaż urządzeń</p> <ul style="list-style-type: none"> • Zamontować w szafach RACK wszystkie dostarczone urządzenia (serwery, pamięci masowe, przełączniki itp.) oraz podzespoły (np. dyski, wkładki SFP). • Zachować porządek i usunąć opakowania oraz zbędne pozostałości po procesie instalacji. <p>2) Okablowanie</p> <ul style="list-style-type: none"> • Podłączyć wszystkie przewody sieciowe w szafie rackowej (miedziane kat. 6 UTP lub światłowodowe), zapewnić potrzebne kable zasilające i listwy. <p>3) Aktualizacja i konfiguracja urządzeń</p> <ul style="list-style-type: none"> • Zaktualizować firmware do najnowszej stabilnej wersji zalecanej przez producenta. • Skonfigurować urządzenia w warstwie fizycznej i logicznej tak, aby były gotowe do pracy zgodnie z ustaleniami z Zamawiającym. • Zainstalować i skonfigurować systemy operacyjne oraz niezbędne oprogramowanie na serwerach. • Uruchomić pamięci masowe i skonfigurować dyski (np. w RAID 10). <p>4) Oznaczenia, testy i dokumentacja</p> <ul style="list-style-type: none"> • Opisać wszystkie porty w sposób trwały i widoczny w szafie rackowej.

		<ul style="list-style-type: none"> • Przeprowadzić testy poprawności działania (szybkość łącz, komunikacja, dostęp do zasobów, redundancja). • Utworzyć dokumentację końcową (parametry, hasła, schematy) i przekazać ją Zamawiającemu. <p>5) Zakres obowiązków Wykonawcy</p> <ul style="list-style-type: none"> • Zainstalować kompletne rozwiązanie, w tym sprzęt i okablowanie, w pomieszczeniu serwerowni. • Włączyć nowe urządzenia do infrastruktury Zamawiającego. • Utworzenie min. 5 maszyn wirtualnych (lub jeśli będzie taka konieczność większej ilości) na dostarczonych serwerach po ustaleniu ich zakresu oraz danych z Zamawiającym. • Zapewnić, że wszystkie elementy (serwery, macierz, NAS, przełączniki) są skonfigurowane i gotowe do użytkowania. • Zrealizować montaż i konfigurację w terminach ustalonych z Zamawiającym, nawet w dni wolne od pracy Urzędu, o ile tak przewiduje umowa. • Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane w oparciu o współpracę z przedstawicielem Zamawiającego. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym. <p>6) Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30. W tym czasie przedstawiciel Wykonawcy:</p> <ul style="list-style-type: none"> • zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. • dokona prezentacji działania systemu dla wyznaczonej osoby przez Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności: <ul style="list-style-type: none"> - zastosowanej technologii serwerów; - zastosowanej technologii pamięci masowej; - systemu backupu.
--	--	---

16 Kursy informatyczne online – 1 kpl.

LP.	OPIS	WYMAGANIA MINIMALNE
1.	Typ kursu	Online (dostęp do platformy) dla minimum 38 pracowników.
2.	Wymagania dodatkowe	<p>1) Osoba lub osoby posiadające wieloletnie doświadczenie dydaktyczne w zakresie wymaganych kursów w obszarach wiedzy wymienionych w bieżącej tabeli.</p> <p>2) Zamawiający wymaga, aby uczestnik każdego szkolenia otrzymał:</p> <ul style="list-style-type: none"> • materiały szkoleniowe w wersji elektronicznej; • wsparcie poszkoleniowe trenera w okresie minimum 14 dni po zakończeniu szkolenia; • certyfikat ukończenia szkolenia. <p>3) Zamawiający wymaga także, aby szkolenia dedykowane dla pracowników jednostki zorganizowane były przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.</p>

3.	Okres dostępu do platformy	Minimum do 30 czerwca 2026 roku.
4.	Zakres merytoryczny szkolenia	<ol style="list-style-type: none"> 1) Wprowadzenie do zagadnień cyberbezpieczeństwa, w tym omówienie celów szkolenia oraz podstawowych pojęć związanych z bezpieczeństwem pracy w środowisku cyfrowym. 2) Socjotechnika jako narzędzie cyberprzestępców, obejmująca: <ul style="list-style-type: none"> • identyfikację podmiotów wykorzystujących techniki socjotechniczne oraz ich motywacje finansowe, • sposoby pozyskiwania i wykorzystywania danych osobowych, • mechanizmy skuteczności socjotechniki, • skutki działań cyberprzestępców dla osób fizycznych i organizacji, • praktyczne zasady ochrony przed kradzieżą tożsamości. 3) Bezpieczeństwo haseł i mechanizmów uwierzytelniania, w tym: <ul style="list-style-type: none"> • dostępność haseł w publicznych bazach danych, • metody weryfikacji wycieków haseł, • czas i metody łamania haseł, w tym pojęcie haseł słownikowych, • zasady tworzenia i bezpiecznego przechowywania haseł, • stosowanie uwierzytelniania dwuskładnikowego. 4) Bezpieczeństwo poczty elektronicznej, obejmujące: <ul style="list-style-type: none"> • zagadnienia związane z fałszowaniem nadawcy (spoofing), • zasady weryfikacji nadawcy wiadomości, • analizę treści, załączników oraz odnośników internetowych, • przegląd najczęściej występujących zagrożeń, • procedury zgłaszania i śledzenia incydentów bezpieczeństwa. 5) Ochronę przed phishingiem, w tym: <ul style="list-style-type: none"> • definicję i charakterystykę phishingu, • analizę przykładowych ataków phishingowych, • zasady czytania adresów URL i nazw domen, • identyfikację pułapek w nazwach domen, • zagadnienia związane z certyfikatami bezpieczeństwa stron internetowych. 6) Bezpieczeństwo stron WWW i przeglądarek internetowych, obejmujące: <ul style="list-style-type: none"> • rolę i konfigurację przeglądarek internetowych, • zagrożenia związane z plikami cookies, • zapamiętywanie haseł w przeglądarce, • ataki typu clickjacking, likejacking oraz tabnabbing, • interpretację ostrzeżeń dotyczących certyfikatów bezpieczeństwa. 7) Ataki socjotechniczne z wykorzystaniem urządzeń fizycznych, w tym: <ul style="list-style-type: none"> • zagrożenia wynikające z użycia nośników danych nieznanego pochodzenia, • wykorzystanie znanych i nieznanych urządzeń w atakach, • ryzyka związane z niebezpiecznymi gadżetami USB, • praktyczne zasady bezpiecznej konfiguracji urządzeń (np. ustawienia autoplay). 8) Ataki realizowane za pośrednictwem telefonu i wiadomości SMS, obejmujące: <ul style="list-style-type: none"> • podszywanie się pod nadawcę (SMS spoofing), • phishing telefoniczny, • scenariusze oszustw typu „na bank”, „na policjanta”, „na wsparcie techniczne”, • zasady reagowania na podejrzane próby i kontakty. 9) Zagrożenia związane z urządzeniami mobilnymi, w tym:

	<ul style="list-style-type: none">• bezpieczeństwo aplikacji mobilnych,• zarządzanie uprawnieniami aplikacji,• smartfon jako potencjalne narzędzie inwigilacji,• metody zabezpieczania urządzeń mobilnych oraz aktualizacji systemowych. <p>10) Zagrożenia związane z sieciami Wi-Fi, obejmujące:</p> <ul style="list-style-type: none">• ryzyka korzystania z publicznych sieci bezprzewodowych,• możliwość tworzenia fałszywych sieci wykradających dane,• zasady bezpiecznego korzystania z sieci Wi-Fi,• zarządzanie zapamiętanymi sieciami na urządzeniach użytkowników. <p>11) Szkolenie powinno obejmować zadania praktyczne oraz testy sprawdzające wiedzę po poszczególnych zakresach tematycznych.</p>
--	--