



---

**Cyberbezpieczny  
Samorząd**

---



## **OPIS PRZEDMIOTU ZAMÓWIENIA**

**Cyberbezpieczny samorząd –  
zakup i montaż sprzętu komputerowego dla Starostwa  
Powiatowego w Żarach**

**WIZ.272.01.2025**



# Cyberbezpieczny Samorząd

## 1. Preambuła

Niniejszy dokument określa szczegółowe wymagania dotyczące dostawy, wdrożenia oraz uruchomienia oprogramowania i infrastruktury sprzętowej w ramach realizacji projektu „Cyberbezpieczny Samorząd” w Starostwie Powiatowym w Żarach.

Projekt ten jest współfinansowany w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2: Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest podniesienie poziomu cyberbezpieczeństwa jednostek samorządu terytorialnego poprzez wdrożenie zaawansowanych rozwiązań technologicznych i organizacyjnych, które zwiększają ochronę danych, minimalizują ryzyko zagrożeń cybernetycznych oraz zapewniają ciągłość działania systemów informacyjnych.

Realizacja projektu odzwierciedla strategiczne podejście do cyfryzacji administracji publicznej, mające na celu wzmocnienie zdolności samorządów lokalnych do przeciwdziałania współczesnym wyzwaniom w zakresie bezpieczeństwa cyfrowego. Wszelkie działania będą podejmowane w zgodzie z krajowymi i europejskimi standardami, w tym w zakresie interoperacyjności, dostępności oraz ochrony danych osobowych.

## 2. Wymagania ogólne

### 2.1. Równoważność oferowanych rozwiązań

W celu zachowania neutralności technologicznej i konkurencyjności Zamawiający dopuszcza zastosowanie rozwiązań równoważnych do wyspecyfikowanych. Za rozwiązanie równoważne uznaje się takie, które pod względem technologii, wydajności i funkcjonalności nie odbiega istotnie od określonych parametrów. Należy przy tym uwzględnić, że cechy unikalne dla danego rozwiązania, takie jak zastrzeżone patenty czy własnościowe technologie, nie podlegają porównaniu. Istotne jest, aby rozwiązanie równoważne zapewniało porównywalną wartość użytkową, realizując te same funkcjonalności w sposób niezakłócający integralności systemu.

Wykonawca proponujący rozwiązanie równoważne zobowiązany jest dostarczyć dokumentację potwierdzającą spełnienie wymagań funkcjonalnych Zamawiającego, w tym wyniki porównań, testów oraz opis możliwości oferowanego rozwiązania w odniesieniu do wyspecyfikowanego.

#### 2.1.1. Oprogramowanie

Implementacja oprogramowania równoważnego musi odbyć się bez zakłóceń w bieżącej pracy Zamawiającego, obejmując migrację niezbędnych danych, szkolenie użytkowników, konfigurację systemu oraz zapewnienie gwarancji i serwisu. Wszelkie działania powinny być realizowane zgodnie z ustalonym harmonogramem i w porozumieniu z Zamawiającym.

W przypadku braku możliwości uzyskania odpowiedniego dostępu do oprogramowania firm trzecich, Zamawiający dopuszcza wymianę oprogramowania pod warunkiem, że:



## Cyberbezpieczny Samorząd

- a) Wykonawca dostarcza i wdraża rozwiązania zastępujące na własny koszt, zgodnie z warunkami licencjonowania określonymi w niniejszym dokumencie.
- b) Migracja danych, obejmująca pełny zakres danych bieżących i archiwalnych, przeprowadzana jest na koszt Wykonawcy i zgodnie z opisem w OPZ.
- c) Wykonawca zapewnia instruktaże stanowiskowe, gwarancję, serwis gwarancyjny, help desk oraz asystę techniczną umożliwiającą płynną obsługę oprogramowania przez pracowników Zamawiającego.
- d) Wymiana oprogramowania nie zakłóca bieżącej pracy Zamawiającego i zapewnia ciągłość operacyjną zgodnie z obowiązującymi terminami, przepisami prawa i procedurami.
- e) Uzgodnienia i konsultacje dotyczące transmisji danych odbywają się w siedzibie Zamawiającego według zatwierdzonego harmonogramu.
- f) Proces migracji obejmuje pełne dane zawarte w poprzednio użytkowanym systemie.
- g) Nowe rozwiązania spełniają wszystkie określone wymagania względem oprogramowania.

### 2.1.2. Infrastruktura sprzętowa

Jeśli w opisie przedmiotu zamówienia wskazano znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, które charakteryzują produkty lub usługi dostarczane przez konkretnego wykonawcę, co mogłoby prowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie mógł opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń, co jest uzasadnione specyfiką przedmiotu zamówienia. W takich przypadkach wszelkie odniesienia należy interpretować z dopiskiem „lub równoważne”.

Gdy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, dopuszcza się rozwiązania równoważne opisywanym, a powyższe odniesienia należy rozumieć z dopiskiem „lub równoważne”.

Przez rozwiązania równoważne Zamawiający rozumie sprzęt o parametrach technicznych i funkcjonalnych co najmniej równych określonym w OPZ. Wykonawca powołujący się na rozwiązania równoważne jest zobowiązany wykazać, że oferowane dostawy lub usługi spełniają wymagania Zamawiającego.

O ile nie zaznaczono inaczej, wszelkie parametry techniczne podane w OPZ należy traktować jako minimalne. Na przykład zapis: „Zainstalowane dwa procesory minimum 12-rdzeniowe klasy x86, min. 3.0GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 207 w teście SPECrate2017\_int\_base, dostępnym na stronie [www.spec.org](http://www.spec.org) dla konfiguracji dwuprocessorowej” należy rozumieć jako:

„Zainstalowane co najmniej dwa procesory, posiadające co najmniej 12 rdzeni, klasy x86, o taktowaniu co najmniej 3.0GHz, umożliwiające osiągnięcie wyniku co najmniej 207 w teście SPECrate2017\_int\_base dla oferowanego serwera, dostępnego na stronie [www.spec.org](http://www.spec.org) w konfiguracji dwuprocessorowej”.



## Cyberbezpieczny Samorząd

### 3. Infrastruktura teleinformatyczna (obszar techniczny)

3.0.1.	Dostarczane urządzenia muszą być fabrycznie nowe (wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostawy) i pochodzić z oficjalnego kanału dystrybucyjnego producenta.
3.0.2.	Zamawiający zastrzega, by dostarczane urządzenia nie były używane przed ich dostawą i odbiorem. Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem).
3.0.3.	Serwery wirtualizacji HCI 1 Nod mają stanowić kompletne rozwiązanie typu Cluster zbudowany wg następującej konfiguracji: a) Cluster hiperkonwergentny (HCI – Hyper-Converged Infrastructure) 3 Nodowy zbudowany z 3 szt. jednostek serwerowych Serwer wirtualizacji HCI 1 Nod (pkt.3.3) wraz z Oprogramowaniem Systemowym typ I (pkt.3.7).

#### 3.1. Urządzenie klasy UTM z licencją na 2 lata

3.1.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją urządzenia typu UTM (Unified Threat Management) z licencją na 2 lata na warunkach określonych w SWZ zwanym dalej systemem lub systemem bezpieczeństwa.
3.1.2.	Klasa produktu: UTM (Unified Threat Management).
3.1.3.	<p>UTM - kompleksowy system bezpieczeństwa, który integruje w jednej platformie kluczowe funkcje ochrony sieciowej i zarządzania bezpieczeństwem, zapewniając kompleksową ochronę infrastruktury IT.</p> <p>System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia.</p> <p>Uwaga: W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Jeżeli realizacja wymagań wymaga dostarczenia odrębnej(-ych) licencji to dostawa licencji stanowi Przedmiot Zamówienia.</p>
3.1.4.	Funkcja Firewall zapewnia pracę w jednym z trzech trybów: a) routera z funkcją NAT, b) transparentnym, c) z monitorowania na porcie SPAN.
3.1.5.	<p>System musi umożliwić budowę min. 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie:</p> <p>a) routingu, b) Firewall'a, c) IPSec VPN, d) antywirus, e) IPS, f) kontroli aplikacji,</p> <p>Uwaga: Powinna istnieć możliwość dedykowania min. 5 administratorów do poszczególnych instancji systemu.</p>



## Cyberbezpieczny Samorząd

3.1.6.	Wsparcie dla protokołów IPv4 oraz IPv6 w zakresie (zakres minimalny): a) Firewall, b) ochrony w warstwie aplikacji, c) protokołów routingu dynamicznego.
	Redundancja, monitoring i wykrywanie awarii
3.1.7.	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS możliwość łączenia w klaster: a) Active-Active, b) Active-Passive,  Uwaga: W obu trybach system firewall musi zapewniać funkcję synchronizacji sesji.
3.1.8.	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych: Tak.
3.1.9.	Monitoring stanu realizowanych połączeń VPN: Tak.
3.1.10.	System musi umożliwiać agregację linków: a) statyczną, b) w oparciu o protokół LACP, c) możliwość tworzenia interfejsów redundantnych.
	Interfejsy
3.1.11.	System realizujący funkcję Firewall: a) min. 10 szt. Gigabit Ethernet RJ-45, b) min. 8 szt. SFP 1 Gbps, c) min. 4 szt. SFP+ 10 Gbps.
3.1.12.	System realizujący funkcję Firewall: a) wbudowany port konsoli szeregowej: Tak, b) gniazdo USB umożliwiające instalację oprogramowania przy użyciu klucza USB: Tak.
3.1.13.	System realizujący funkcję Firewall musi umożliwiać skonfigurowanie: a) min. 200 interfejsów wirtualnych definiowanych jako VLAN'y w oparciu o standard 802.1Q.
3.1.14.	System wyposażony w zasilanie AC: Tak.
3.1.15.	Parametry wydajnościowe: a) Firewall: obsługa min. 3 mln jednoczesnych połączeń oraz min. 100 tys. nowych połączeń na sekundę, b) przepustowość Stateful Firewall: min. 35 Gbps (dla pakietów 512 B), c) przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: min. 6.0 Gbps., d) wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128: min. 30 Gbps., e) wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix: min. 5 Gbps., f) wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – min. 2.5 Gbps., g) wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http: min. 3 Gbps..
3.1.16.	Funkcje Systemu bezpieczeństwa: a) kontrola dostępu: zaporą ogniową klasy Stateful Inspection, b) kontrola Aplikacji: Tak, c) poufność transmisji danych: i. połączenia szyfrowane IPSec VPN, ii. SSL VPN, d) ochrona przed malware: Tak, e) ochrona przed atakami: Intrusion Prevention System, f) kontrola stron WWW: Tak,



## Cyberbezpieczny Samorząd

	<p>g) kontrola zawartości poczty: Antyspam dla protokołów SMTP, POP3,</p> <p>h) zarządzanie pasmem (QoS, Traffic shaping): Tak,</p> <p>i) mechanizmy ochrony przed wyciekiem poufnej informacji (DLP): Tak,</p> <p>j) dwuskładnikowe uwierzytelnianie: wykorzystaniem tokenów sprzętowych lub programowych.</p> <p>Uwaga: Wymagane min. 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</p> <p>k) inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu:</p> <ol style="list-style-type: none"><li>HTTP (w tym HTTP/2),</li><li>SMTP,</li><li>FTP,</li><li>POP3.</li></ol> <p>l) funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system,</p> <p>m) rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).</p> <p>Uwaga: W ramach systemu ochrony muszą być zrealizowane wszystkie wymienione w pkt. funkcje. Zamawiający dopuszcza rozwiązanie, w którym wymienione w pkt. funkcje mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych.</p>
	<b>Polityki, Firewall</b>
3.1.17.	Polityka Firewall musi uwzględniać (zakres minimalny): <ol style="list-style-type: none"><li>adresy IP,</li><li>użytkowników,</li><li>protokoły,</li><li>usługi sieciowe,</li><li>aplikacje lub zbiory aplikacji,</li><li>reakcje zabezpieczeń,</li><li>rejestrowanie zdarzeń.</li></ol>
3.1.18.	Realizacja translacji adresów NAT: <ol style="list-style-type: none"><li>źródłowego i docelowego,</li><li>translację PAT,</li><li>translację jeden do jeden oraz jeden do wielu,</li><li>ALG (Application Level Gateway): dla protokołu SIP.</li></ol>
3.1.19.	Możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
3.1.20.	Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: <ol style="list-style-type: none"><li>kategorie URL,</li><li>adresy IP.</li></ol>
3.1.21.	Inne: <ol style="list-style-type: none"><li>możliwość filtrowania ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe,</li><li>możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</li></ol>



## Cyberbezpieczny Samorząd

3.1.22.	<p>Rozwiązanie lub jego element musi umożliwiać integrację z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych w procesie budowania polityk kontroli dostępu:</p> <ul style="list-style-type: none"><li>a) Amazon Web Services (AWS),</li><li>b) Microsoft Azure,</li><li>c) Cisco ACI,</li><li>d) Google Cloud Platform (GCP),</li><li>e) OpenStack,</li><li>f) VMware NSX,</li><li>g) Kubernetes.</li></ul>
	<b>Połączenia VPN</b>
3.1.23.	<p>Konfiguracja połączeń typu IPSec VPN (zakres min. funkcjonalności):</p> <ul style="list-style-type: none"><li>a) wsparcie dla IKE v1 oraz v2,</li><li>b) obsługa szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM),</li><li>c) obsługa protokołu Diffie-Hellman grup 19, 20,</li><li>d) wsparcie dla pracy w topologii Hub and Spoke oraz Mesh,</li><li>e) tworzenie połączeń typu Site-to-Site oraz Client-to-Site,</li><li>f) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,</li><li>g) możliwość wyboru tunelu przez protokoły:<ul style="list-style-type: none"><li>i. dynamicznego routingu (np. OSPF),</li><li>ii. routingu statycznego,</li></ul></li><li>h) wsparcie typów uwierzytelniania: pre-shared key, certyfikat,</li><li>i) możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu,</li><li>j) możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu,</li><li>k) obsługa mechanizmów:<ul style="list-style-type: none"><li>i. IPSec NAT Traversal,</li><li>ii. DPD,</li><li>iii. Xauth,</li></ul></li><li>l) wbudowany mechanizm „Split tunneling” dla połączeń Client-to-Site.</li></ul>
3.1.24.	<p>Konfigurację połączeń typu SSL VPN (zakres min. funkcjonalności):</p> <ul style="list-style-type: none"><li>a) praca w trybie Portal - dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki.</li></ul> <p>Uwaga: W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.</p> <ul style="list-style-type: none"><li>b) praca w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</li></ul> <p>Uwaga: Wymagane jest, aby producent rozwiązania posiadał w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie VPN musi być dostępne jako opcja i nie jest wymagane w implementacji rozwiązania.</p>
3.1.25.	<p>Routing i obsługa łączy WAN:</p> <ul style="list-style-type: none"><li>a) routing statyczny: Tak,</li><li>b) obsługa Policy Based Routingu: Tak, w tym wybór trasy w zależności od:<ul style="list-style-type: none"><li>i. adresu źródłowego,</li><li>ii. protokołu sieciowego,</li></ul></li></ul>



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>iii. oznaczeń Type of Service w nagłówkach IP,</li><li>c) obsługa protokołów dynamicznego routingu w oparciu o protokoły:<ul style="list-style-type: none"><li>i. RIPv2 (w tym RIPng),</li><li>ii. OSPF (w tym OSPFv3),</li><li>iii. BGP,</li><li>iv. PIM,</li></ul></li><li>d) możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu,</li><li>e) ECMP (Equal cost multi-path): Tak, wybór wielu równoważnych tras w tablicy routingu,</li><li>f) BFD (Bidirectional Forwarding Detection): Tak,</li><li>g) monitoring dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</li></ul>
3.1.26.	<p>Funkcje SD-WAN (Software Defined Wide Area Network):</p> <ul style="list-style-type: none"><li>a) możliwość wykorzystania protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN,</li><li>b) wymagane wsparcie zarówno dla interfejsów fizycznych jak i wirtualnych (w tym VLAN, IPSec).</li></ul>
3.1.27.	<p>Zarządzanie pasmem:</p> <ul style="list-style-type: none"><li>a) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie:<ul style="list-style-type: none"><li>i. maksymalnej i gwarantowanej ilości pasma,</li><li>ii. oznaczanie DSCP</li><li>iii. wskazanie priorytetu ruchu.</li></ul></li><li>b) możliwość określania pasma dla poszczególnych aplikacji.</li><li>c) możliwość zdefiniowania pasma dla wybranych użytkowników niezależnie od ich adresu IP,</li><li>d) możliwość zarządzania pasmem dla wybranych kategorii URL.</li></ul>
	<b>Ochrona przed malware</b>
3.1.28.	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
3.1.29.	<p>Silnik antywirusowy musi zapewniać skanowanie następujących protokołów:</p> <ul style="list-style-type: none"><li>a) HTTP,</li><li>b) HTTPS,</li><li>c) FTP,</li><li>d) POP3,</li><li>e) IMAP,</li><li>f) SMTP,</li><li>g) CIFS.</li></ul>
3.1.30.	<p>System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR.</p> <p>Uwaga: W przypadku archiwów zagnieżdżonych możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.</p>
3.1.31.	Możliwość blokowania i logowania archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
3.1.32.	<p>System musi dysponować sygnaturami do ochrony urządzeń mobilnych (min. dla systemu operacyjnego Android).</p> <p>Uwaga: Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p>





## Cyberbezpieczny Samorząd

3.1.33.	<p>Inne:</p> <ul style="list-style-type: none"><li>a) współpraca z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze</li></ul> <p>Uwaga: Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze,</p> <ul style="list-style-type: none"><li>b) możliwość usuwania aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików,</li><li>c) możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta rozwiązania.</li></ul> <p>Uwaga: Jeżeli realizacja wymagania wymaga dostarczenia odrębnej(-ych) licencji to dostawa licencji nie stanowi Przedmiotu Zamówienia.</p> <ul style="list-style-type: none"><li>d) możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</li></ul>
3.1.34.	<p>Ochrona przed atakami:</p> <ul style="list-style-type: none"><li>a) ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych,</li><li>b) ochrona przed atakami na aplikacje pracujące na niestandardowych portach,</li><li>c) baza sygnatur ataków zawiera min. 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez Administratora,</li><li>d) możliwość definiowania własnych wyjątków oraz własnych sygnatur przez Administratora,</li><li>e) wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</li><li>f) mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym, ochrona przed (zakres minimalny):<ul style="list-style-type: none"><li>i. CSS,</li><li>ii. SQL Injecton,</li><li>iii. Trojany,</li><li>iv. Exploity,</li><li>v. Roboty.</li></ul></li><li>g) możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http,</li><li>h) wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet: Tak,</li><li>i) możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej</li></ul> <p>Uwaga: Mechanizmy ochrony IPS nie mogą działać globalnie.</p>
3.1.35.	<p>Kontrola aplikacji</p> <ul style="list-style-type: none"><li>a) funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów (nie bazując jedynie na wartościach portów TCP/UDP),</li><li>b) Baza Kontroli Aplikacji musi zawierać min. 2000 sygnatur i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez Administratora,</li><li>c) kontrola aplikacji chmurowych pod względem wykonywanych czynności (np.: pobieranie, wysyłanie plików) (zakres minimalny):<ul style="list-style-type: none"><li>i. Facebook,</li><li>ii. Google Docs,</li><li>iii. Dropbox,</li></ul></li></ul>



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>d) Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa:<ul style="list-style-type: none"><li>i. proxy,</li><li>ii. P2P,</li></ul></li><li>e) Administrator musi mieć możliwość definiowania wyjątków oraz własnych sygnatur,</li><li>f) możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021),</li><li>g) możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</li></ul>
3.1.36.	<p>Kontrola WWW</p> <ul style="list-style-type: none"><li>a) rozwiązanie (lub jego moduł kontroli WWW) korzystające z bazy zawierającej min. 40 milionów adresów URL pogrupowanych w kategorie tematyczne,</li></ul> <p>Uwaga w ramach filtra WWW dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <ul style="list-style-type: none"><li>b) filtr WWW musi umożliwiać:<ul style="list-style-type: none"><li>i. dostarczanie kategorii stron zabronionych prawem (np.: Hazard),</li><li>ii. statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwalać definiować strony z zastosowaniem wyrażeń regularnych (Regex),</li><li>iii. wykonanie akcji typu „Warning” – tj. ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony,</li></ul></li><li>c) możliwość nadpisywania kategorii oraz tworzenia wyjątków (białe/czarne listy dla adresów URL) przez Administratora,</li><li>d) wbudowana funkcja SafeSearch (lub inne równoważne zaimplementowane algorytmy) przeciwdziałająca pojawianiu się niechcianych treści w wynikach wyszukiwarek (zakres minimalny):<ul style="list-style-type: none"><li>i. Google,</li><li>ii. Yahoo,</li></ul></li><li>e) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW,</li><li>f) możliwość definiowania, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</li></ul>
	Uwierzytelnianie użytkowników, zarządzanie, logowanie
3.1.37.	<p>System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą haseł:</p> <ul style="list-style-type: none"><li>a) statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,</li><li>b) statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,</li><li>c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li></ul> <p>Uwaga: System musi umożliwić zastosowanie w tym procesie uwierzytelniania dwuskładnikowego.</p>
3.1.38.	<p>Możliwość budowy architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.</p> <p>Uwaga: Zamawiający dopuszcza zastosowanie innych mechanizmów np. RADIUS, API lub SYSLOG w tym procesie.</p>
3.1.39.	<p>Wymagane uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP (lub inny równoważny).</p>



## Cyberbezpieczny Samorząd

3.1.40.	<p>Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania</p> <p>Uwaga: Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.</p>
3.1.41.	<p>Możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</p>
3.1.42.	<p>Współpraca z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3.</p> <p>Uwaga: Rozwiązanie musi umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p>
3.1.43.	<p>Wbudowane API dające możliwość zarządzania przez systemy firm trzecich</p> <p>Uwaga: Producent w takim przypadku udostępnia pełną dokumentację API.</p>
3.1.44.	<p>Wbudowane narzędzia diagnostyczne umożliwiające (zakres minimalny):</p> <ul style="list-style-type: none"><li>a) ping,</li><li>b) traceroute,</li><li>c) podglądu pakietów,</li><li>d) monitorowanie procesowania sesji,</li><li>e) monitorowanie stanu sesji firewall.</li></ul>
3.1.45.	<p>Inne:</p> <ul style="list-style-type: none"><li>a) możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</li><li>b) możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</li></ul>
3.1.46.	<p>Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze.</p> <p>Uwaga: Zamawiający dopuszcza rozwiązanie w oparciu o zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. Jeżeli realizacja wymagań wymaga dostarczenia odrębnej(-ych) licencji to dostawa licencji stanowi Przedmiotu Zamówienia.</p>
3.1.47.	<p>W ramach logowania element systemu pełniący funkcję Firewall musi zapewniać przekazywanie danych o:</p> <ul style="list-style-type: none"><li>a) zaakceptowanym ruchu,</li><li>b) blokowanym ruchu,</li><li>c) aktywności administratorów,</li><li>d) zużyciu zasobów,</li><li>e) stanie pracy systemu</li></ul> <p>Uwaga: Wymagana możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p>
3.1.48.	<p>Inne dot. procesu logowania:</p> <ul style="list-style-type: none"><li>a) logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa,</li><li>b) możliwość włączenia logowania per reguła w polityce firewall.</li></ul>
3.1.49.	<p>Możliwość logowania do serwera SYSLOG: Tak.</p>



## Cyberbezpieczny Samorząd

	<p>Uwaga: W przypadku przesyłania SYSLOG do zewnętrznych systemów, możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
	Serwisy i licencje
3.1.50.	<p>Jeżeli Zamawiający nie zdefiniował inaczej w powyższych wymaganiach, to:</p> <p>w przypadku, gdy do korzystania z aktualnych baz funkcji ochronnych producenta rozwiązania i serwisów wymagane są licencje, w tym wymienione wcześniej oraz obejmujące zakres:</p> <ul style="list-style-type: none"><li>a) Kontrola Aplikacji,</li><li>b) IPS,</li><li>c) Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych, co najmniej dla systemu operacyjnego Android),</li><li>d) Analiza typu Sandbox cloud,</li><li>e) Antyspam,</li><li>f) Web Filtering,</li><li>g) Bazy reputacyjne adresów IP/domen,</li></ul> <p>to dostarczenie niezbędnych licencji w wymaganym zakresie stanowi część Przedmiotu Zamówienia i musi być zapewnione na okres min. 24 miesięcy.</p> <p>Uwaga: Jeżeli realizacja wymagań Zamawiającego wymaga dostarczenia odrębnych licencji, ich dostawa również stanowi integralną część Przedmiotu Zamówienia i musi obejmować okres min. 24 miesięcy.</p>
3.1.51.	Ilość: 1 komplet.
	Gwarancja oraz wsparcie
3.1.52.	<p>System objęty serwisem gwarancyjnym przez okres: zadeklarowany przez Wykonawcę polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (Advanced Hardware Replacement).</p> <p>Uwaga: W ramach tego serwisu musi być zapewniony dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 przez producenta rozwiązania w okresie gwarancyjnym.</p>
3.1.53.	<p>Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie Zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji.</p> <p>Uwaga: Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów przez Zamawiającego, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.</p>
3.1.54.	<p>Rozszerzone wsparcie serwisowe</p> <p>Rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu min. 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy.</p> <p>Uwaga: Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7</p>



## Cyberbezpieczny Samorząd

	Wymagania powinny być potwierdzone dokumentami.
3.1.55.	<p>Wymagane oświadczenia:</p> <ul style="list-style-type: none"><li>a) oświadczenie producenta lub autoryzowanego dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej),</li><li>b) certyfikat ISO 9001 podmiotu serwisującego,</li><li>c) wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).</li></ul>
3.1.56.	<p>Na potwierdzenie, że oferowane Urządzenie aktywne sieciowe spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć następujące dokumenty:</p> <ul style="list-style-type: none"><li>a) opis proponowanego rozwiązania potwierdzający, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego urządzenia wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.</li></ul>
3.1.57.	<p>W zakresie instalacji i konfiguracji urządzeń Wykonawca powinien zapewnić:</p> <ul style="list-style-type: none"><li>a) ustalenie z Zamawiającym terminu przeprowadzenia prac,</li><li>b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia,</li><li>c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce),</li><li>d) fizyczną instalację urządzeń aktywnych w szafach dystrybucyjnych 19", uwzględniającą podłączenie do zasilania 230V oraz wymaganego okablowania,</li><li>e) konfigurację urządzenia zgodnie z wytycznymi Zamawiającego:<ul style="list-style-type: none"><li>i. rejestracja urządzenia / serwisów,</li><li>ii. konfiguracja portu WAN,</li><li>iii. konfiguracja portów LAN (do 5 podsieci),</li><li>iv. konfiguracja VLAN (do 5 podsieci),</li><li>v. konfiguracja Profili Bezpieczeństwa (1 per moduł),</li><li>vi. konfiguracja Polityk Firewall (maks. 10 polityk),</li><li>vii. konfiguracja przekierowań portów (do 5 portów),</li><li>viii. konfiguracja VPN (Ipsec),</li><li>ix. dodanie użytkowników (do 5 userów),</li><li>x. konfiguracja monitorowania stanu urządzenia oraz tuneli VPN,</li><li>xi. konfiguracja mechanizmów redundancji urządzeń w trybie Active-Active i Active-Passive,</li><li>xii. wdrożenie podstawowych reguł bezpieczeństwa z funkcjami antywirusowymi, IPS oraz filtrowaniem stron internetowych (3 polityki),</li><li>xiii. konfiguracja zewnętrznej komunikacji SYSLOG oraz SNMP dla monitorowania urządzenia,</li></ul></li><li>f) zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego.</li></ul>
3.1.58.	<p>Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom:</p> <ul style="list-style-type: none"><li>a) dostawa: formalnemu odbiorowi podlega dostawa do Zamawiającego w ilościach określonych w pkt.3.1.51,</li><li>b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzenia u Zamawiającego zgodnie z wykazem czynności określonym w pkt.3.1.57.</li></ul>



## Cyberbezpieczny Samorząd

### 3.2. Zarządzalny skalowalny przełącznik sieciowy 24x GE wraz z 2 letnią gwarancją

3.2.1.	<p>Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją zarządzalnego skalowalnego przełącznika sieciowego wraz z min. 2 letnią gwarancją na warunkach określonych w SWZ zwany dalej Przełącznikiem.</p> <p>Uwaga: W ramach postępowania Zamawiający wymaga dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. Zamawiający wymaga, aby dostarczony Przełącznik był kompatybilny z systemem bezpieczeństwa opisanym w pkt.3.1. Urządzenie klasy UTM, oraz aby zarządzanie elementami systemu odbywało się z poziomu jednego panelu zarządzania.</p>
3.2.2.	Klasa produktu: zarządzalny przełącznik sieciowy.
3.2.3.	<p>Interfejsy sieciowe:</p> <ul style="list-style-type: none"><li>a) min. 24 porty GE (Gigabit Ethernet) RJ-45,</li><li>b) min. 4 porty 10 GE SFP+</li></ul> <p>Uwaga: Zamawiający nie dopuszcza portów typu combo, wymagany jest, aby Przełącznik dysponował niezależnymi interfejsami sieciowymi.</p>
3.2.4.	<p>Zarządzanie:</p> <ul style="list-style-type: none"><li>a) wbudowany port konsoli szeregowej: Tak,</li><li>b) zarządzanie poprzez:<ul style="list-style-type: none"><li>i. command line (w tym poprzez SSH),</li><li>ii. graficzny interfejs z wykorzystaniem przeglądarki (HTTPS),</li></ul></li><li>c) wsparcie dla SNMP w wersjach 1-3,</li><li>d) funkcja zarządzania pozwalająca na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami,</li><li>e) funkcja aktualizacji oprogramowania przez TFTP/FTP i/lub za pomocą GUI,</li><li>f) funkcja backupu konfiguracji z poziomu GUI i/lub poprzez CLI (TFTP/FTP),</li><li>g) funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li><li>h) możliwość definiowania ról administratorów z możliwością określenia trybu dostępu do wybranych części konfiguracji,</li><li>i) funkcja automatycznego wykonywania rewizje konfiguracji.</li></ul>
3.2.5.	<p>Parametry wydajnościowe:</p> <ul style="list-style-type: none"><li>a) przepustowość:<ul style="list-style-type: none"><li>i. min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach),</li><li>ii. min. 190 Mpps,</li></ul></li><li>b) tablica adresów MAC: min. 32k wpisów,</li><li>c) opóźnienie wprowadzane przez przełącznik: poniżej max. 2 mikrosekund.</li></ul>
3.2.6.	<p>Wymagane funkcjonalności:</p> <ul style="list-style-type: none"><li>a) automatycznej negocjacji prędkości i duplexu dla połączeń: Tak,</li><li>b) Jumbo Frames: Tak,</li><li>c) obsługa protokołów/algorytmów:<ul style="list-style-type: none"><li>i. 802.1d (Spanning Tree),</li><li>ii. 802.1w (Rapid Spanning Tree),</li></ul></li></ul>



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>iii. 802.1s (Multiple Spanning Tree),</li><li>d) agregacja portów: zgodna ze standardem 802.3ad,</li><li>e) VLAN: min. 4000 VLAN'ów (zgodne ze standardem 802.1Q),</li><li>f) routing statyczny: Tak,</li><li>g) Port-mirroring: Tak,</li><li>h) uwierzytelnianie:<ul style="list-style-type: none"><li>i. Uwierzytelnianie 802.1x na poziomie portu,</li><li>ii. Uwierzytelnianie 802.1x w oparciu o adres MAC,</li></ul></li><li>i) w ramach 802.1x<ul style="list-style-type: none"><li>i. wsparcie dla dedykowanego VLAN dla gości (guest VLAN),</li><li>ii. wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia,</li><li>iii. wsparcie dla dynamicznego przypisywania VLAN,</li></ul></li><li>j) obsługa protokołu sFlow: Tak.</li></ul>
3.2.7.	<p>Wymagane funkcjonalności dla integracji z systemem centralnego zarządzania / NAC (Network Access Control) – urządzenia muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler)(tzw. port extender lub element leaf w architekturze spine-leaf).</p> <p>Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:</p> <ul style="list-style-type: none"><li>a) centralne zarządzanie konfiguracją Przełącznika,</li><li>b) aktualizacja oprogramowania realizowana z systemu centralnego zarządzania,</li><li>c) centralne zarządzanie sieciami VLAN,</li><li>d) blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u,</li></ul> <p>W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.</p>
3.2.8.	Ilość: 3 szt.
	Gwarancja oraz wsparcie
3.2.9.	Gwarancja: przez okres zadeklarowany przez Wykonawcę polegająca na naprawie lub wymianie urządzenia w przypadku jego wadliwości.
3.2.10.	Dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w okresie gwarancyjnym.
3.2.11.	Wsparcie techniczne: w trybie 24x7.
3.2.12.	<p>Na potwierdzenie, że oferowany Przełącznik spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć następujące dokumenty:</p> <ul style="list-style-type: none"><li>a) opis proponowanego rozwiązania potwierdzający, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego urządzenia wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.</li></ul>
3.2.13.	<p>W zakresie instalacji i konfiguracji urządzeń Wykonawca powinien zapewnić:</p> <ul style="list-style-type: none"><li>a) ustalenie z Zamawiającym terminu przeprowadzenia prac,</li><li>b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia,</li><li>c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce),</li><li>d) fizyczną instalację urządzeń w szafach dystrybucyjnych 19", uwzględniając podłączenie do zasilania 230V oraz wymaganego okablowania,</li><li>e) konfigurację urządzenia zgodnie z wytycznymi Zamawiającego:<ul style="list-style-type: none"><li>i. konfiguracja portów/agregacji z rozwiązaniem UTM (pkt.3.1.),</li><li>ii. rejestracja oraz aktualizacja urządzenia,</li></ul></li></ul>





## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>iii. konfiguracja VLAN,</li><li>iv. stworzenie połączenia z UTM (pkt.3.1.) tworząc bezpieczny system,</li><li>v. weryfikacja działania VLAN na portach Przełącznika,</li><li>vi. weryfikacja konfiguracji portów / sieci,</li><li>vii. weryfikacja poprawności polityk,</li><li>viii. weryfikacja konfiguracji pod kątem dobrych praktyk,</li><li>ix. przegląd logów pod kątem zagrożeń,</li></ul> <p>f) zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego.</p>
3.2.14.	<p>Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom:</p> <ul style="list-style-type: none"><li>a) dostawa: formalnemu odbiorowi podlega dostawa do Zamawiającego w ilościach określonych w pkt.3.2.8,</li><li>b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzenia u Zamawiającego zgodnie z wykazem czynności określonym w pkt.3.2.13.</li></ul>
3.2.15.	<p>Wymagania dotyczące produktów podwójnego zastosowania</p> <p>W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.</p>

### 3.3. Serwer wirtualizacji HCI 1 Nod z 2 letnią gwarancją

3.3.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Serwera wirtualizacji HCI 1 Nod na warunkach określonych w SWZ.
3.3.2.	<p>Obudowa:</p> <ul style="list-style-type: none"><li>a) typu Rack do instalacji w standardowej szafie RACK 19",</li><li>b) szyny umożliwiające wysunięcie serwera z szafy stelażowej w komplecie,</li><li>c) ilość wnęk dla dysków twardych SSD/HDD/NVMe hot plug 2,5" umożliwiającą montaż dysków opisanych przez Zamawiającego w pkt.3.3.6,</li><li>d) zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek lub inne równoważne) uniemożliwiającego fizyczny dostęp do dysków twardych.</li></ul>
3.3.3.	<p>Płyta główna:</p> <ul style="list-style-type: none"><li>a) dwuprocesorowa,</li><li>b) wyprodukowana i zaprojektowana przez producenta serwera,</li><li>c) możliwość instalacji procesorów min. 60-rdzeniowych,</li><li>d) zainstalowany moduł TPM 2.0,</li><li>e) min. 6 szt. slotów PCI Express min. generacji min. 5,</li><li>f) min. 32 sztuki gniazd pamięci RAM,</li><li>g) obsługa min. 8TB pamięci RAM DDR5,</li><li>h) wsparcie dla technologii (zakres minimalny):<ul style="list-style-type: none"><li>i. Memory Scrubbing,</li><li>ii. ECC,</li></ul></li></ul>





## Cyberbezpieczny Samorząd

	<p>iii. SDDC,</p> <p>i) możliwość instalacji min. dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express).</p>
3.3.4.	<p>Procesory:</p> <p>a) zainstalowane: min. 2 szt. min. 16-rdzeniowe,</p> <p>b) architektura x86_64,</p> <p>c) taktowanie bazowe: min. 2.8GHz,</p> <p>d) osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 490 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów).</p> <p>Uwaga: Wynik musi być opublikowany na stronie <a href="http://spec.org/cpu2017/results/cpu2017.html">http://spec.org/cpu2017/results/cpu2017.html</a></p>
3.3.5.	<p>Pamięć RAM:</p> <p>a) zainstalowane: min. 512GB,</p> <p>b) typ: DDR5 Registered 5600MT/s</p> <p>Uwaga: Pamięci obsadzone w sposób gwarantujący najwyższą możliwość wydajność.</p>
3.3.6.	<p>Zainstalowane dyski twarde:</p> <p>a) min. 2 szt. dysków NVMe PCIe 4 min. 480GB M.2 podpięte do sprzętowego kontrolera RAID 1,</p> <p>b) min. 4 szt. dysków NVMe PCIe 5 min. 3.84TB Read-Intensive Hot-Plug.</p>
3.3.7.	<p>Interfejsy zintegrowane:</p> <p>a) zintegrowana karta graficzna ze złączem VGA,</p> <p>b) min. 2 szt. portów USB 3.0,</p> <p>c) min. 1 szt. portów USB wewnętrzny,</p> <p>d) możliwość instalacji min. 1 szt. portu serial RS232: opcjonalnie.</p> <p>Uwaga: Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.</p>
3.3.8.	<p>Interfejsy sieciowe:</p> <p>a) interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:</p> <p>i. min. 1 szt. 1Gbit Base-T,</p> <p>ii. min. 4 szt. 25Gbit SFP28,</p> <p>Uwaga: Możliwość uzyskania dwóch interfejsów min. 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe.</p>
3.3.9.	<p>Zasilanie i chłodzenie:</p> <p>a) redundantne zasilacze hotplug o sprawności min. 96% (tzw. klasa Titanium) o mocy min. 900W: 2 szt.,</p> <p>b) redundantne wentylatory hotplug.</p>
3.3.10.	<p>Zarządzanie:</p> <p>a) zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:</p>



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>i. niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera,</li><li>ii. dedykowana karta LAN 1Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym,</li><li>iii. dostęp poprzez przeglądarkę Web, SSH,</li><li>iv. zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii,</li><li>v. zarządzanie alarmami (zdarzenia poprzez SNMP),</li><li>vi. możliwość przejęcia konsoli tekstowej,</li><li>vii. możliwość przekierowania konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM),</li><li>viii. obsługa serwerów proxy (autentykacja),</li><li>ix. obsługa VLAN,</li><li>x. możliwość konfiguracji parametru Max. Transmission Unit (MTU),</li><li>xi. wsparcie dla protokołu SSDP,</li><li>xii. Obsługa protokołów TLS 1.2, SSL v3,</li><li>xiii. obsługa protokołu LDAP,</li><li>xiv. synchronizacja czasu poprzez protokół NTP,</li><li>xv. możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej,</li></ul> <p>b) dostarczone oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające:</p> <ul style="list-style-type: none"><li>i. konfigurację kontrolera RAID,</li><li>ii. instalację systemów operacyjnych,</li><li>iii. zdalne zarządzanie,</li><li>iv. diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);</li></ul> <p>c) wbudowana karta zarządzająca (lub zainstalowana) pamięć flash lub rozwiązanie równoważne dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN,</p> <p>Uwaga: Serwer musi posiadać możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera.</p>
3.3.11.	<p>Wymagane wsparcie dla systemów SSO (zakres minimalny):</p> <ul style="list-style-type: none"><li>a) SSO zgodnie z pkt. 3.7,</li><li>b) Microsoft Windows Server 2022, 2019,</li><li>c) VMWare vSphere 8.0,</li><li>d) Suse Linux Enterprise Server 15,</li><li>e) Red Hat Enterprise Linux 9, 8,</li><li>f) Microsoft Hyper-V Server 2019.</li></ul>
3.3.12.	<p>Pozostałe wymagania:</p> <ul style="list-style-type: none"><li>a) elementy, z których zbudowane jest serwer muszą być produktami producenta tego serwera lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA,</li><li>b) serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego wymagane oświadczenie wykonawcy lub producenta z chwilą dostawy.</li></ul>



## Cyberbezpieczny Samorząd

3.3.13.	Oprogramowanie SSO: zainstalowane Oprogramowanie systemowe typ I (SSO) zgodnie z wymaganiami opisanymi przez Zamawiającego w pt.3.7.
3.3.14.	Ilość: 3 szt.
3.3.15.	<p>Gwarancja: zadeklarowana przez Wykonawcę - w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia.</p> <ul style="list-style-type: none"><li>a) naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis,</li><li>b) możliwość zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu,</li><li>c) bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywno dla oferowanego serwera</li></ul> <p>Uwaga: Jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniony w ofercie Wykonawcy,</p> <ul style="list-style-type: none"><li>d) możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.</li></ul>
3.3.16.	<p>Dokumentacja, inne</p> <ul style="list-style-type: none"><li>a) ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera,</li><li>b) możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.</li></ul>
3.3.17.	<p>Do czynności Wykonawcy w ramach montażu i uruchomienia serwera należy:</p> <ul style="list-style-type: none"><li>a) ustalenie z Zamawiającym terminu przeprowadzenia prac,</li><li>b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia,</li><li>c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce),</li><li>d) instalacja urządzenia zgodnie ze specyfikacjami produktu, w tym m.in. zamontowanie w szafach dystrybucyjnych,</li><li>e) instalacja SSO zgodnie z pkt.3.7,</li><li>f) oznakowanie sprzętu naklejką,</li><li>g) zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego.</li></ul>
3.3.18.	<p>Na potwierdzenie, że oferowany Serwer backupu spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć do oferty następujące dokumenty:</p> <ul style="list-style-type: none"><li>a) opis proponowanego rozwiązania potwierdzający, że oferowany Serwer wirtualizacji HCI 1 Nod spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.</li><li>b) opis proponowanego rozwiązania potwierdzający, że oferowany SSO spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, rodzaju licencji oferowanego rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.</li></ul>
3.3.19.	<p>Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom:</p> <ul style="list-style-type: none"><li>a) dostawa: formalnemu odbiorowi podlega dostawa w ilościach określonych w pkt.3.3.14,</li><li>b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzeń zgodnie z wykazem czynności określonym w pkt.3.3.17.</li></ul>



## Cyberbezpieczny Samorząd

### 3.4. Serwer backupu danych z 2 letnią gwarancją

3.4.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją Serwera backupu danych na warunkach określonych w SWZ.
3.4.2.	Obudowa: <ul style="list-style-type: none"><li>a) typu Rack do instalacji w standardowej szafie RACK 19",</li><li>b) szyny umożliwiające wysunięcie serwera z szafy stelażowej w komplecie,</li><li>c) ilość wnęk dla dysków twardych Hotplug 3,5" umożliwiającą montaż dysków opisanych przez Zamawiającego w pkt.3.4.6,</li><li>d) zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek lub inne równoważne) uniemożliwiającego fizyczny dostęp do dysków twardych.</li></ul>
3.4.3.	Płyta główna: <ul style="list-style-type: none"><li>a) dwuprocesorowa,</li><li>b) wyprodukowana i zaprojektowana przez producenta serwera,</li><li>c) możliwość instalacji procesorów min. 60-rdzeniowych,</li><li>d) zainstalowany moduł TPM 2.0,</li><li>e) min. 6 szt. slotów PCI Express min. generacji min. 5,</li><li>f) min. 32 sztuki gniazd pamięci RAM,</li><li>g) obsługa min. 8TB pamięci RAM DDR5,</li><li>h) wsparcie dla technologii (zakres minimalny):<ul style="list-style-type: none"><li>i. Memory Scrubbing,</li><li>ii. ECC,</li><li>iii. SDDC,</li></ul></li><li>i) możliwość instalacji min. dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express).</li></ul>
3.4.4.	Procesory: <ul style="list-style-type: none"><li>a) zainstalowane: min. 1 szt. min. 8-rdzeniowe,</li><li>b) architektura x86_64,</li><li>c) taktowanie bazowe: min. 2.6GHz,</li><li>d) osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów).</li></ul> <p>Uwaga: Wynik musi być opublikowany na stronie <a href="http://spec.org/cpu2017/results/cpu2017.html">http://spec.org/cpu2017/results/cpu2017.html</a>.</p>
3.4.5.	Pamięć RAM: <ul style="list-style-type: none"><li>a) zainstalowane: min. 128GB,</li><li>b) typ: DDR5 Registered 4800MT/s.</li></ul>
3.4.6.	Zainstalowane dyski twarde: <ul style="list-style-type: none"><li>a) min. 2 szt. 3,5" SSD SATA o pojemności min. 960GB hot-plug typu Read-Intensive,</li><li>b) min. 10 szt. 3,5" HDD SAS 7200 obr./min hot-plug o pojemności min. 12TB,</li><li>c) możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4.</li></ul>
3.4.7.	Kontrolery I/O: <ul style="list-style-type: none"><li>b) zainstalowany kontroler SAS RAID dla dysków wewnętrznych posiadający min. 2GB pamięci cache, obsługujący poziomy RAID (zakres minimalny): 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania.</li></ul>
3.4.8.	Interfejsy zintegrowane: <ul style="list-style-type: none"><li>a) zintegrowana karta graficzna ze złączem VGA,</li></ul>



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>b) min. 2 szt. portów USB 3.0,</li><li>c) min. 1 szt. portów USB wewnętrzny,</li><li>d) możliwość instalacji min. 1 szt. portu serial RS232: opcjonalnie.</li></ul> <p>Uwaga: Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.</p>
3.4.9.	<p>Interfejsy sieciowe:</p> <ul style="list-style-type: none"><li>a) interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:<ul style="list-style-type: none"><li>i. min. 4 szt. 1Gbit Base-T,</li></ul></li></ul> <p>Uwaga: Możliwość uzyskania dwóch interfejsów min. 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe,</p> <ul style="list-style-type: none"><li>b) interfejsy LAN zainstalowane w slotach PCI-e:<ul style="list-style-type: none"><li>i. min. 2 szt. 10Gbit SFP+ obsadzone wkładkami MMF LC każdy.</li></ul></li></ul>
3.4.10.	<p>Zasilanie i chłodzenie:</p> <ul style="list-style-type: none"><li>a) redundantne zasilacze hotplug o sprawności min. 96% (tzw. klasa Titanium) o mocy min. 900W: 2 szt.,</li><li>b) redundantne wentylatory hotplug.</li></ul>
3.4.11.	<p>Zarządzanie:</p> <ul style="list-style-type: none"><li>a) zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:<ul style="list-style-type: none"><li>i. niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera,</li><li>ii. dedykowana karta LAN 1Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym,</li><li>iii. dostęp poprzez przeglądarkę Web, SSH,</li><li>iv. zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii,</li><li>v. zarządzanie alarmami (zdarzenia poprzez SNMP),</li><li>vi. możliwość przejścia konsoli tekstowej,</li><li>vii. możliwość przekierowania konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM),</li><li>viii. obsługa serwerów proxy (autentykacja),</li><li>ix. obsługa VLAN,</li><li>x. możliwość konfiguracji parametru Max. Transmission Unit (MTU),</li><li>xi. wsparcie dla protokołu SSDP,</li><li>xii. Obsługa protokołów TLS 1.2, SSL v3,</li><li>xiii. obsługa protokołu LDAP,</li><li>xiv. synchronizacja czasu poprzez protokół NTP,</li><li>xv. możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej,</li></ul></li><li>b) dostarczone oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające:<ul style="list-style-type: none"><li>i. konfigurację kontrolera RAID,</li><li>ii. instalację systemów operacyjnych,</li><li>iii. zdalne zarządzanie,</li></ul></li></ul>



## Cyberbezpieczny Samorząd

	<p>iv. diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);</p> <p>c) wbudowana karta zarządzająca (lub zainstalowana) pamięć flash lub rozwiązanie równoważne dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN,</p> <p>Uwaga: Serwer musi posiadać możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera.</p>
3.4.12.	<p>Wymagane wsparcie dla systemów SSO (zakres minimalny):</p> <ul style="list-style-type: none"><li>a) Microsoft Windows Server 2022, 2019,</li><li>b) VMWare vSphere 8.0,</li><li>c) Suse Linux Enterprise Server 15,</li><li>d) Red Hat Enterprise Linux 9, 8,</li><li>e) Microsoft Hyper-V Server 2019.</li></ul>
3.4.13.	<p>Pozostałe wymagania:</p> <ul style="list-style-type: none"><li>a) elementy, z których zbudowane jest serwer muszą być produktami producenta tego serwera lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA,</li><li>b) serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego wymagane oświadczenie wykonawcy lub producenta z chwilą dostawy.</li></ul>
3.4.14.	<p>Ilość: 1 szt.</p>
3.4.15.	<p>Gwarancja: zadeklarowana przez Wykonawcę w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia.</p> <ul style="list-style-type: none"><li>a) naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis,</li><li>b) możliwość zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu,</li><li>c) bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywno dla oferowanego serwera</li></ul> <p>Uwaga: Jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniony w ofercie Wykonawcy,</p> <ul style="list-style-type: none"><li>d) możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.</li></ul>
3.4.16.	<p>Dokumentacja, inne</p> <ul style="list-style-type: none"><li>a) ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera,</li><li>b) możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.</li></ul>
3.4.17.	<p>Do czynności Wykonawcy w ramach montażu i uruchomienia serwera należy:</p> <ul style="list-style-type: none"><li>a) ustalenie z Zamawiającym terminu przeprowadzenia prac,</li><li>b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia,</li><li>c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce),</li></ul>



## Cyberbezpieczny Samorząd

	d) instalacja urządzenia zgodnie ze specyfikacjami produktu, w tym m.in. zamontowanie w szafach dystrybucyjnych, e) oznakowanie sprzętu naklejką, f) zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego.
3.4.18.	Na potwierdzenie, że oferowany Serwer backupu spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć do oferty następujące dokumenty: a) opis proponowanego rozwiązania potwierdzający, że oferowany Serwer backupu spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.
3.4.19.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: a) dostawa: formalnemu odbiorowi podlega dostawa w ilościach określonych w pkt.3.4.14, b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzeń zgodnie z wykazem czynności określonym w pkt.3.4.17.

### 3.5. Urządzenie NAS (Network Attached Storage)

3.5.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją urządzenia typu NAS (Network Attached Storage) na warunkach określonych w SWZ.
3.5.2.	Klasa produktu: NAS (Network Attached Storage).
3.5.3.	Procesor: czterordzeniowy min. 64-bitowy min. 3.3GHz.
3.5.4.	Obudowa: RACK 19" - wraz z kompletem szyn umożliwiającym zamontowanie w szafie RACK.
3.5.5.	Pamięć RAM: zainstalowane min. 32GB DDR4 ECC,  Uwaga: Pamięć RAM zgodna z listą kompatybilności producenta NAS.
3.5.6.	Liczba zatok HDD: min. 12 szt.
3.5.7.	Obsługiwane dyski twarde: a) 3.5" SATA HDD / 2.5" SATA SSD – Hot Swap.
3.5.8.	Zainstalowane dyski twarde: a) min. 6 szt. 3.5" SATA HDD min. 20TB o parametrach nie gorszych niż: i. prędkość obrotowa: min. 7200 RPM, ii. MTTF: min. 2.500.000, iii. obciążenie roczne: min. 500 TB, iv. gwarancja producenta dysku  Uwaga: Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera. Dyski muszą być zgodne z listą kompatybilności producenta NAS.
3.5.9.	Porty na karty rozszerzeń: min. 1 szt. Gen3.
3.5.10.	LAN: a) min. 1 szt. 1GbE RJ-45, b) min. 1 szt. 10GbE RJ-45, c) min. 1 szt. 10GbE SFP+  Uwaga: W celu realizacji wymagania Zamawiający dopuszcza możliwość zastosowanie dodatkowych kart sieciowych z listy kompatybilności producenta NAS.





## Cyberbezpieczny Samorząd

3.5.11.	Port USB: Tak (3.2).
3.5.12.	Redundantne zasilanie: a) zasilacz o mocy min. 350W.
3.5.13.	Obsługiwane tryby RAID: JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny.
3.5.14.	Pozostałe wymagania: a) mechanizm szyfrowania sprzętowego: Tak, b) uprawnienia: lista kontroli dostępu systemu Windows (ACL).
3.5.15.	Usługa katalogowa: a) możliwość połączenia się z serwerami Windows® AD/LDAP  Uwaga: Usługa musi umożliwiać użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station.
3.5.16.	Funkcje bezpieczeństwa: a) obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów): Tak, dla folderów współdzielonych i migawek, b) zaporę sieciową, c) szyfrowanie: i. folderu współdzielonego, ii. całego woluminu, iii. SMB, FTP (przez SSL/TLS), SFTP, d) automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów: i. HTTP, ii. HTTPS, iii. SMB, iv. SSH, v. Telnet, vi. FTP, e) obsługa Let's Encrypt, f) HTTPS (dostosowywane mechanizmy szyfrowania), g) dwuetapowa weryfikacja logowania (2FA).
3.5.17.	Oprogramowanie do kopii zapasowej: a) kopia zapasowa całego systemu Windows (bare-metal) oraz przywracanie w trybie bare-metal, b) kopia zapasowa środowisk MacOS: Tak, pełna zgodność z plikami użytkownika, c) kopia zapasowa maszyn wirtualnych: VMware i Microsoft Hyper-V, d) kopia zapasowa serwerów fizycznych: Windows, Linux, e) obsługa deduplikacji, kopii przyrostowych, kompresji oraz szyfrowania, f) obsługa wielu wersji i retencji dla plików kopii zapasowej, g) możliwość wyzwalania kopii zapasowej według harmonogramu (automatyzacja zadań), h) obsługa klastra przełączania awaryjnego Hyper-V dla zapewnienia wysokiej dostępności, i) automatyczna weryfikacja utworzonych kopii zapasowych poprzez symulowane odtworzenie (np. w formie wideo lub maszyny wirtualnej). j) centralne zarządzanie kopiami zapasowymi z jednej konsoli administracyjnej, k) konfiguracja nowych oraz edycja istniejących zadań backupowych dla wielu urządzeń (w tym harmonogramy, wersje i retencja), l) portal użytkownika do przywracania danych kopii zapasowej (bez konieczności posiadania uprawnień administratora), m) delegowanie uprawnień do zarządzania kopią zapasową oraz przywracaniem dla użytkowników z ograniczonymi uprawnieniami,





## Cyberbezpieczny Samorząd

	<p>n) kopia zapasowa usług chmur publicznych: Microsoft 365 oraz Google Workspace.</p> <p>Zgodność z oferowanym serwerem, potwierdzona przez producenta urządzenia.</p> <p>Uwaga: Zgodność współpracy oprogramowania do kopii zapasowej z oferowanym NAS. Oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Jeżeli realizacja wymagania wymaga dostarczenia odrębnej(-ych) licencji to dostawa tych licencji stanowi Przedmiot Zamówienia.</p>
3.5.18.	<p>Oprogramowanie:</p> <ul style="list-style-type: none"><li>a) nowoczesny system plików zapewniający:<ul style="list-style-type: none"><li>i. obsługę migawek,</li><li>ii. generowanie sum kontrolnych,</li><li>iii. lustrzane kopie metadanych w celu zapewnienia integralności danych biznesowych,</li><li>iv. ustawienie limitu dla folderów współdzielonych.</li><li>v. szybkie klonowanie całych folderów udostępnionych,</li></ul></li><li>b) aplikacja do realizacji chmury prywatnej:<ul style="list-style-type: none"><li>i. konsola administratora zarządzana z GUI,</li><li>ii. agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS,</li><li>iii. udostępnianie zasobów serwera NAS,</li><li>iv. synchronizację i tworzenie kopii zapasowych podłączonych urządzeń,</li><li>v. obsługa pracy z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny),</li><li>vi. wsparcie dla wersjonowana oraz jednoczesnej edycję plików biurowych przez wielu użytkowników,</li></ul></li></ul> <p>Uwaga: Realizacja wymagania poprzez darmową aplikację bez jakichkolwiek opłat cyklicznych.</p> <ul style="list-style-type: none"><li>c) klaster wysokiej dostępności (HA):<ul style="list-style-type: none"><li>i. możliwość stworzenia klastra HA z dwóch identycznych serwerów NAS,</li><li>ii. automatyczne przełączanie dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego,</li></ul></li><li>d) kopia zapasowa danych serwera:<ul style="list-style-type: none"><li>i. tworzenie kopii zapasowej na zewnętrzne dyski twarde (USB),</li><li>ii. kopia zapasowa do chmur publicznych,</li><li>iii. kopia zapasowa na serwer rsync,</li></ul></li><li>e) obsługa migawek:<ul style="list-style-type: none"><li>i. min. 1024 migawek na folder współdzielony,</li><li>ii. min. 50 000 migawek na cały system,</li></ul></li><li>f) funkcja serwera VPN:<ul style="list-style-type: none"><li>i. obsługa protokołów: OpenVPN, L2TP/IPSec oraz PPTP.</li><li>ii. wsparcie dla min. 40 jednoczesnych połączeń.</li></ul></li></ul>
3.5.19.	Ilość: 2 szt.
3.5.20.	Gwarancja: zadeklarowana przez Wykonawcę.
3.5.21.	<p>Gwarancja obejmuje:</p> <ul style="list-style-type: none"><li>a) Gwarancja dotyczy również takich podzespołów sprzętowych takich jak pamięć RAM pkt.3.5.5, dyski twarde pkt. 3.5.8, karty sieciowe pkt. 3.5.10 oraz inne komponenty dostarczone w raz z serwerem NAS.</li></ul>



## Cyberbezpieczny Samorząd

3.5.22.	Do czynności Wykonawcy w ramach montażu i uruchomienia serwera należy: a) ustalenie z Zamawiającym terminu przeprowadzenia prac, b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia, c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce), d) instalacja urządzenia zgodnie ze specyfikacjami produktu, w tym m.in. zamontowanie w szafach dystrybucyjnych, e) oznakowanie sprzętu naklejką, f) zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego.
3.5.23.	Na potwierdzenie, że oferowany Serwer backupu spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć do oferty następujące dokumenty: a) opis proponowanego rozwiązania potwierdzający, że oferowane urządzenie spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.
3.5.24.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: a) dostawa: formalnemu odbiorowi podlega dostawa w ilościach określonych w pkt.3.5.19, b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzeń zgodnie z wykazem czynności określonym w pkt.3.5.22.

### 3.6. Urządzenie typu UPS moc. 10kVA

3.6.1.	Zakres Przedmiotu zamówienia obejmuje dostawę, montaż wraz z uruchomieniem i konfiguracją urządzenia typu UPS moc min. 10kVA z 2 letnią gwarancją na warunkach określonych w SWZ zwany dalej UPS.
3.6.2.	Klasa produktu: podwójna konwersja UPS online.
3.6.3.	Moc znamionowa: min. 10 kVA / 10kW.
3.6.4.	Architektura/Technologia: beztransformatorowa o podwójnej konwersji.
3.6.5.	Konfiguracja wejścia/wyjścia: a) 3-fazowe wejście / 3-fazowe wyjście: Tak, b) 3-fazowe wejście / 1-fazowe wyjście: Tak.
3.6.6.	Nominalne napięcie wejściowe (AC): 400 V.
3.6.7.	Zakres napięcia wejściowego: od min. 320 V do min 450 V.
3.6.8.	Częstotliwość nominalna: 50/60 Hz.
3.6.9.	Zakres częstotliwości wejściowej: od min. 40Hz do min. 70Hz.
3.6.10.	Współczynnik mocy wejściowej: $\geq$ min 0,96 przy pełnym obciążeniu.
3.6.11.	Nominalny prąd wejścia podstawowego: min. 25A.
3.6.12.	Typ gniazda wejściowego: połączenia stałe (3f, N, PE).
3.6.13.	Nominalne napięcie wyjściowe: 400 V.
3.6.14.	Prąd wyjściowy przy 400VAC: min. 15A.
3.6.15.	Autonomia: min. 12 minut dla 10kW**  <u>Uwaga:</u> Zamawiający dopuszcza wydłużenie czasu podtrzymania poprzez dołożenie dodatkowych modułów bateryjnych. Dobór ilości baterii, w zależności od wymagań opisanych przez Zamawiającego, należy do Wykonawcy.



## Cyberbezpieczny Samorząd

	** Dane podane dla temp. otoczenia 25°C.
3.6.16.	Żywotność akumulatorów: min. 3 - 5 lat (wg EUROBAT).
3.6.17.	Współczynnik mocy obciążenia: 1.
3.6.18.	<p>Komunikacja i zarządzanie:</p> <ul style="list-style-type: none"><li>a) wyjścia bezpotencjałowe do sygnalizacji stanów alarmowych: opcjonalnie,</li><li>b) slot na karty komunikacyjne: Tak, obsługa protokołów:<ul style="list-style-type: none"><li>i. SNMP,</li><li>ii. Modbus.</li></ul></li><li>c) karta komunikacyjna w celu zdalnego monitoringu UPS: Tak</li></ul> <p>Uwaga: Komunikacja przez SNMP oraz Modbus lub BACnet. Do karty komunikacyjnej należy dołączyć czujnik środowiskowy monitorujący wilgotność i temperaturę w pomieszczeniu UPS. Dostawa karty komunikacyjnej wraz z czujnikiem stanowi przedmiot zamówienia.</p>
3.6.19.	<p>Montaż:</p> <ul style="list-style-type: none"><li>a) możliwość montażu UPS w szafie rackowej: Tak.</li><li>b) miejsce instalacji baterii: Moduły bateryjne (zalecany montaż w szafie 19").</li></ul>
3.6.20.	<p>Inne wymagane:</p> <ul style="list-style-type: none"><li>a) dedykowany bypass zewnętrzny: Tak (przeznaczony do instalacji w szafie 19"),</li><li>b) wejście EPO (Emergency Power Off): Tak,</li><li>c) zimny start: Tak.</li></ul>
3.6.21.	<p>Ilość: 1 szt.</p> <p>Wyposażenie dodatkowe:</p> <ul style="list-style-type: none"><li>a) Karta opisana w pkt. 3.6.15: 1 szt.</li></ul>
3.6.22.	Gwarancja: zadeklarowana przez Wykonawcę
3.6.23.	<p>Gwarancja obejmuje:</p> <ul style="list-style-type: none"><li>a) naprawę lub wymianę UPS w przypadku jego awarii w miejscu jego instalacji,</li><li>b) dostęp do aktualizacji oprogramowania (firmware) przez okres gwarancji,</li><li>c) wsparcie techniczne dostępne w trybie 24x7 (24 godziny na dobę, 7 dni w tygodniu) w języku polskim.</li></ul>
3.6.24.	<p>Na potwierdzenie, że oferowany UPS spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć następujące dokumenty:</p> <ul style="list-style-type: none"><li>a) opis proponowanego rozwiązania potwierdzający, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, marki oraz modelu (numerów katalogowych) oferowanego urządzenia wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.</li></ul>
3.6.25.	<p>W zakresie instalacji i konfiguracji urządzeń Wykonawca powinien zapewnić:</p> <ul style="list-style-type: none"><li>a) ustalenie z Zamawiającym terminu przeprowadzenia prac,</li><li>b) rozpakowanie urządzenia, sprawdzenie, czy nie wystąpiły uszkodzenia,</li><li>c) sprawdzenie warunków wymaganych do pracy urządzenia (temperatura, zasilanie, dostępne miejsce),</li><li>d) fizyczną instalację urządzeń i podłączenie do zasilania oraz wymaganego okablowania,</li><li>e) konfigurację urządzenia zgodnie z wytycznymi Zamawiającego poprzez usługę uruchomienia tzw. StartUp oferowaną przez producenta lub autoryzowanego partnera serwisowego dla zaproponowanego modelu, która obejmuje<ul style="list-style-type: none"><li>i. instalacja w szafie rack 19",</li></ul></li></ul>



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>ii. połączenie z istniejącą infrastrukturą elektryczną,</li><li>iii. Testy funkcjonalne obejmujące:<ul style="list-style-type: none"><li>▪ uruchomienie UPS,</li><li>▪ kalibrację i konfigurację parametrów systemowych,</li></ul></li><li>iv. weryfikacja działania baterii oraz obciążenia,</li><li>v. szkolenie podstawowe dla użytkowników.</li><li>f) dostarczenie raportu z instalacji i konfiguracji,</li><li>g) dostarczenie certyfikatu zgodności oraz dokumentacji technicznej.</li></ul>
3.6.26.	<p>Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom:</p> <ul style="list-style-type: none"><li>a) dostawa: formalnemu odbiorowi podlega dostawa do Zamawiającego w ilościach określonych w pkt.3.6.21,</li><li>b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja urządzenia u Zamawiającego zgodnie z wykazem czynności określonym w pkt.3.6.25.</li></ul>

### 3.7. Oprogramowanie Systemowe typ I (SSO)

3.7.1.	Oprogramowanie Systemowe typ I - Serwerowy System Operacyjny (SSO).
3.7.2.	Oprogramowanie systemowe typ I (SSO) musi spełniać wymagania minimalne opisane w pkt. od 3.7. oraz pochodzić z najnowszej linii produktowej Producenta.
3.7.3.	<p>Licencja SSO musi uprawniać do zainstalowania SSO w środowisku fizycznym oraz umożliwiać zainstalowanie min. 100 szt. instancji wirtualnych tego SSO.</p> <p>Uwaga: Licencja SSO musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze opisanym w pkt.3.3.</p>
3.7.4.	Licencja dożywotnia nie może być ograniczona czasowo.
3.7.5.	<p>Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.</p> <ul style="list-style-type: none"><li>a) możliwość wykorzystania min. 320 logicznych procesorów oraz co najmniej min. 4TB pamięci RAM w środowisku fizycznym,</li><li>b) możliwość wykorzystywania min. 64 procesorów wirtualnych oraz min. 1TB pamięci RAM i dysku o pojemności do 64TB min. przez każdy wirtualny serwerowy system operacyjny,</li><li>c) możliwość budowania klastrów składających się z min. 64 węzłów, z możliwością uruchamiania min. 100 maszyn wirtualnych,</li><li>d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,</li><li>e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,</li><li>f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,</li><li>g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,</li><li>h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading)</li><li>i) wbudowane wsparcie instalacji i pracy na wolumenach, które:</li></ul>



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>i. pozwalają na zmianę rozmiaru w czasie pracy systemu,</li><li>ii. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</li><li>iii. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</li><li>iv. umożliwiają zdefiniowanie list kontroli dostępu (ACL),</li><li>j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,</li><li>k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</li><li>l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,</li><li>m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,</li><li>n) wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li></ul>
3.7.6.	Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ul style="list-style-type: none"><li>a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li><li>b) dotykowy umożliwiający sterowanie dotykem na monitorach dotykowych.</li></ul>
3.7.7.	Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
3.7.8.	Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
3.7.9.	Pozostałe wymagania: <ul style="list-style-type: none"><li>c) mechanizmy logowania w oparciu o:<ul style="list-style-type: none"><li>i. Login i hasło,</li><li>ii. Karty z certyfikatami (smartcard),</li><li>iii. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</li></ul></li><li>d) możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:<ul style="list-style-type: none"><li>i. określonych grup użytkowników,</li><li>ii. zastosowanej klasyfikacji danych,</li><li>iii. centralnych polityk dostępu w sieci,</li><li>iv. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.</li></ul></li><li>e) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play),</li><li>f) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,</li><li>g) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,</li><li>h) pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management),</li><li>i) wsparcie dla środowisk Java i .NET Framework 4.x (możliwość uruchomienia aplikacji działających we wskazanych środowiskach).</li></ul>
3.7.10.	Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: <ul style="list-style-type: none"><li>a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</li><li>b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na</li></ul>



## Cyberbezpieczny Samorząd

	<p>tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:</p> <ul style="list-style-type: none"><li>i. podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,</li><li>ii. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,</li><li>iii. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.</li></ul> <p>c) zdalna dystrybucja oprogramowania na stacje robocze,</p> <p>d) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,</p> <p>e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:</p> <ul style="list-style-type: none"><li>i. dystrybucję certyfikatów poprzez http,</li><li>ii. konsolidację CA dla wielu lasów domeny,</li><li>iii. automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,</li><li>iv. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.</li></ul> <p>f) szyfrowanie plików i folderów,</p> <p>g) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),</p> <p>h) możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,</p> <p>i) serwis udostępniania stron WWW,</p> <p>j) wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>k) wsparcie dla algorytmów Suite B (RFC 4869),</p> <p>l) wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,</p> <p>m) wbudowane mechanizmy wirtualizacji pozwalające na uruchamianie do min. 100 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:</p> <ul style="list-style-type: none"><li>i. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,</li><li>ii. obsługi ramek typu jumbo frames dla maszyn wirtualnych,</li><li>iii. obsługi 4-KB sektorów dysków,</li><li>iv. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra</li></ul> <p>n) 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>o) wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath),</p> <p>p) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,</p> <p>q) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,</p> <p>r) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p>
--	---





## Cyberbezpieczny Samorząd

### 3.8. Usługa poczty elektronicznej

3.8.1.	Zakres Przedmiotu zamówienia obejmuje realizację usługi poczty elektronicznej dla 120 użytkowników przez okres 24 m-cy na warunkach określonych w SWZ.
3.8.2.	Funkcjonalność główna: kompleksowa platforma pracy grupowej, łącząca funkcje poczty elektronicznej, kalendarza, współdzielonych dokumentów i komunikacji biznesowej dla 120 użytkowników.
3.8.3.	Funkcje poczty e-mail: <ul style="list-style-type: none"><li>a) obsługa kont e-mail dla min. 120 użytkowników,</li><li>b) dostęp przez IMAP/POP3/SMTP oraz Webmail,</li><li>c) wsparcie dla kalendarzy, kontaktów, zadań oraz notatek z synchronizacją między urządzeniami za pomocą standardów CalDAV i CardDAV,</li><li>d) wsparcie dla ActiveSync lub innych protokołów do synchronizacji danych poczty, kalendarzy i kontaktów na urządzeniach mobilnych</li><li>e) możliwość zarządzania folderami pocztowymi i regułami wiadomości,</li><li>f) obsługa aliasów e-mail oraz grup dystrybucyjnych.</li></ul>
3.8.4.	Kalendarze i współdzielenie zasobów: <ul style="list-style-type: none"><li>a) współdzielenie kalendarzy z możliwością podglądu dostępności użytkowników,</li><li>b) zarządzanie zasobami organizacyjnymi (np. sale konferencyjne, sprzęt),</li><li>c) funkcja zapraszania uczestników na spotkania oraz potwierdzania udziału,</li><li>d) integracja z zewnętrznymi systemami kalendarzowymi (np. Outlook, Google Calendar) za pomocą standardu iMIP.</li></ul>
3.8.5.	Komunikacja wewnętrzna: <ul style="list-style-type: none"><li>a) wsparcie dla czatu i wymiany wiadomości w czasie rzeczywistym,</li><li>b) funkcja komunikacji zespołowej z możliwością tworzenia kanałów lub grup konwersacyjnych,</li><li>c) udostępnianie plików i dokumentów w ramach komunikacji,</li><li>d) możliwość integracji z platformami do wideokonferencji wspierającymi standard WebRTC.</li></ul>
3.8.6.	Funkcje współpracy (collaboration): <ul style="list-style-type: none"><li>a) możliwość tworzenia i współdzielenia dokumentów biurowych (edytor tekstowy, arkusze kalkulacyjne, prezentacje),</li><li>b) obsługa pracy grupowej nad dokumentami z wersjonowaniem,</li><li>c) wsparcie dla współpracy w czasie rzeczywistym z użytkownikami wewnętrznymi i zewnętrznymi (np. poprzez linki z uprawnieniami dostępu do odczytu i edycji),</li><li>d) synchronizacja plików między użytkownikami i urządzeniami.</li></ul>
3.8.7.	Bezpieczeństwo: <ul style="list-style-type: none"><li>a) szyfrowanie transmisji danych (TLS/SSL) oraz zawartości wiadomości e-mail,</li><li>b) wbudowane mechanizmy antywirusowe i antyspamowe,</li><li>c) ochrona przed phishingiem oraz nieautoryzowanym dostępem,</li><li>d) możliwość tworzenia reguł bezpieczeństwa (np. blokowanie załączników).</li><li>e) dwustopniowa autoryzacja (2FA) dla logowania użytkowników.</li></ul>
3.8.8.	Dostępność i mobilność: <ul style="list-style-type: none"><li>a) dostęp do usług z poziomu urządzeń mobilnych (Android/iOS) oraz komputerów stacjonarnych (PC/Mac),</li><li>b) synchronizacja danych za pomocą protokołu ActiveSync,</li><li>c) możliwość pracy w trybie offline z późniejszą synchronizacją danych.</li><li>d) aplikacje klienckie kompatybilne z przeglądarkami internetowymi (zakres minimalny): Chrome, Firefox, Safari, Edge.</li></ul>
3.8.9.	Skalowalność i zarządzanie:



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>a) zarządzanie użytkownikami i uprawnieniami z poziomu graficznej konsoli administracyjnej,</li><li>b) możliwość skalowania systemu dla większej liczby użytkowników,</li><li>c) możliwość instalacji rozwiązania w architekturze High Availability (HA) dla zapewnienia nieprzerwanego dostępu do usług,</li><li>d) monitorowanie działania systemu oraz generowanie raportów (logi aktywności użytkowników).</li></ul>
3.8.10.	Wsparcie i integracja: <ul style="list-style-type: none"><li>a) integracja z Active Directory/LDAP dla centralnego zarządzania kontami użytkowników,</li><li>b) dostęp do wsparcia technicznego producenta przez okres 24 miesięcy,</li><li>c) regularne aktualizacje oprogramowania w ramach dostarczonej licencji,</li><li>d) możliwość migracji danych z innych rozwiązań pocztowych (np. Exchange, IMAP/POP3).</li></ul>
3.8.11.	Zakres usługi: dla min. 120 użytkowników na okres min. 24 m-cy.
3.8.12.	Gwarancja i wsparcie: przez okres zadeklarowany przez Wykonawcę - obejmujące aktualizacje oprogramowania oraz monitorowanie usługi.
3.8.13.	Gwarancja - pozostałe wymagania: <ul style="list-style-type: none"><li>a) reakcja na zgłoszenia w trybie 24/7,</li><li>b) możliwość rozbudowy do 200 kont oraz opcji dodatkowych, takich jak VoIP czy zaawansowane funkcje antyspamowe.</li></ul>
3.8.14.	Na potwierdzenie, że oferowana usługa spełnia wymagania określone przez Zamawiającego Wykonawca zobowiązany jest dołączyć następujące dokumenty: <ul style="list-style-type: none"><li>a) opis proponowanego rozwiązania potwierdzający, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego. Wykonawca zobowiązany jest do wskazania producenta, rodzaju licencji oferowanego rozwiązania wraz ze wszystkimi niezbędnymi komponentami dla spełnienia oczekiwanych wymagań.</li></ul>
3.8.15.	W zakresie instalacji i konfiguracji urządzeń Wykonawca powinien zapewnić: <ul style="list-style-type: none"><li>a) ustalenie z Zamawiającym terminu przeprowadzenia prac,</li><li>b) instalacja na serwerze dedykowanym lub w architekturze klastrowej (patrz pkt.3.0.3),</li><li>c) konfiguracja, uruchomienie oraz testy funkcjonalności min. poczty (pkt.3.8.3), komunikacji wew. (pkt.3.8.5),</li><li>d) szkolenie dla administratora oraz użytkowników końcowych (min. 4 godziny szkolenia on-site),</li><li>e) dostarczenie raportu z instalacji i konfiguracji.</li></ul>
3.8.16.	Etapy realizacji dostaw oraz prac wdrożeniowych podlegające formalnym odbiorom: <ul style="list-style-type: none"><li>a) dostawa: formalnemu odbiorowi podlega dostawa do Zamawiającego w ilościach określonych w pkt.3.8.11,</li><li>b) instalacja i konfiguracja: formalnemu odbiorowi podlega instalacja i konfiguracja usługi u Zamawiającego zgodnie z wykazem czynności określonym w pkt.3.8.15.</li></ul>