



Cyberbezpieczny Samorząd

Załącznik 1 – Opis Przedmiotu Zamówienia

Celem zamówienia jest zwiększenie poziomu cyberbezpieczeństwa Zamawiającego, poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych. Celem jest wdrożenia mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni.

W wyniku podjętych działań przyczyniających się do sprawnego i bezpiecznego działania systemów informatycznych, podniesie się poziom cyberbezpieczeństwa.

W celu wzmocnienia odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych konieczny jest zakup sprzętu, oprogramowania i usług informatycznych w obszarze cyberbezpieczeństwa jako kompleksowego i efektywnego rozwiązania.

Skutkiem realizacji będzie skuteczne zabezpieczenie systemów informatycznych przed cyberprzestępczością w kontekście: ochrony danych osobowych (RODO), potencjalnej utraty danych, ujawnienia wrażliwych danych osobom nieuprawnionym albo umożliwienia atakującym zniszczenia dokumentów lub danych, co zapewni ciągłość pracy oraz zwiększy poczucie bezpieczeństwa.

Zamówienia zostało podzielone na dwie części.

OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI I:

Przedmiot dotyczy kompleksowego rozwiązania, obejmującego:

1. Usługi wsparcia realizowane przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa.
2. Zakup, instalacja i konfiguracja urządzenia ochrony brzegu sieci UTM.
3. Zakup oraz konfiguracja serwera wirtualizacji wraz z systemem operacyjnym oraz licencjami do maszyn wirtualnych, licencji dostępowych. Usługa migracji systemów i wdrożenia wirtualizacji na serwerach.
4. Dostawa i instalacja serwera NAS wraz z systemem archiwizacji. Konfiguracja systemu archiwizacji danych.
5. Instalacja kontrolera domeny AD oraz wdrożenie domeny Microsoft Active Directory z migracją profili użytkowników.
6. Zakup wraz z instalacją i konfiguracją zarządzalnego przełącznika sieciowego.
7. Zakup zasilaczy awaryjnych UPS do stacji roboczych – 10 szt.
8. Zakup zasilaczy awaryjnych UPS do serwerów – 2 szt.

Wykonawca w ramach dostaw ww. sprzętów i wdrożenia ww. usług, zobowiązany jest do wykonania:

1. dostawy sprzętu komputerowego i oprogramowania wraz z ich instalacją i konfiguracją;
2. przeniesienia istniejących usług oraz wdrożenia nowych (opis poniżej);



Cyberbezpieczny Samorząd

3. zapewnienia wsparcia powdrożeniowego w zakresie utrzymania infrastruktury i cyberbezpieczeństwa;
4. przygotowania dokumentacji powykonawczej zawierającej między innymi: zestawienie numerów seryjnych dostarczonych urządzeń, wykorzystanie adresacji IP, specyfikację sprzętu, konfigurację sieci (schemat fizyczny oraz logiczny) oraz środowiska wirtualnego;
5. przeprowadzenia testów poprawności działania zainstalowanego sprzętu oraz oprogramowania;
6. przeprowadzenia podstawowego szkolenie dla administratora Zamawiającego pod kątem zarządzania wdrożonymi usługami oraz sprzętem.

I. Usługi wsparcia realizowane przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa:

Przedmiotem zapytania jest wsparcie zespołu Zamawiającego w z zapewnieniu cyberbezpieczeństwa w zakresie:

- konfiguracji monitoringu stanu cyberbezpieczeństwa w tym zdarzeń występujących w środowisku informatycznym Zamawiającego
- konfiguracji ochrony przed atakami (w szczególności ransomware, DDOS, włamania do zasobów serwerów i stacji roboczych);
- aktualizacji konfiguracji na urządzeniach sieciowych i serwerach
- podejmowania szybkich działań w reakcji na incydenty bezpieczeństwa w celu zminimalizowania ich skutków.
- analizy informacji oraz identyfikacja zdarzenia, zagrożenia i incydentu;
- podjęcia działania w przypadku wystąpienia zdarzenia, w celu minimalizacji efektu ataku.
- analizy przypadku po ustaniu niebezpieczeństwa.

Sposób i tryb wykonania przedmiotu zapytania.

Usługa powinna być wykonywana w sposób zdalny.

Harmonogram i czas trwania wykonania przedmiotu zapytania.

Przedmiot zapytania powinien być wykonany w ciągu 12 miesięcy od daty podpisania umowy.

Wymagania dotyczące jakości usług (SLA)

Poniżej zostały określone parametry jakościowe usługi wykonywanej w obszarze technicznym

- Identyfikacja i ocena istotności zdarzenia, ustalenie szczegółów zdarzenia i potencjalnych skutków oraz wstępna kwalifikacja – do 4 godzin;
- Czas podjęcia działań w środowisku JST w odpowiedzi na wykryte zdarzenie (ograniczenie skutków) i dalsza ocena – do 6 godzin;
- Podjęcie działań naprawczych (przywracanie usług) – od 4 godziny od powiadomienia;
- Analiza skutków zdarzenia, wnioski, dostosowanie nowych działań w postaci m.in. szkoleń/newsletterów itd. – do 15 dni;



Cyberbezpieczny Samorząd

II. Zakup, instalacja i konfiguracja urządzenia ochrony brzegu sieci UTM.

	Wymagane minimalne parametry techniczne
Wymagania Ogólne	<p>Dostarczony system bezpieczeństwa musi zapewniać 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. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <p>Firewall.</p> <p>Ochrony w warstwie aplikacji.</p> <p>Protokołów routingu dynamicznego.</p>
Redundancja, monitoring i wykrywanie awarii	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.</p>
Interfejsy, Zasilanie: Dysk,	<p>System realizujący funkcję Firewall musi dysponować minimum:</p> <p>10 portami Gigabit Ethernet RJ-45.</p> <p>System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</p> <p>W ramach systemu Firewall powinna być możliwość zdefiniowania co</p>



Cyberbezpieczny Samorząd

	<p>najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>System musi być wyposażony w zasilanie AC.</p>
Parametry wydajnościowe:	<p>W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.</p> <p>Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.</p> <p>Wydajność szyfrowania IPsec VPN nie mniej niż 6 Gbps.</p> <p>Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.</p> <p>Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.</p> <p>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.</p>
Funkcje Systemu Bezpieczeństwa:	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <p>Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</p> <p>Kontrola Aplikacji.</p> <p>Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN.</p> <p>Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.</p> <p>Ochrona przed atakami - Intrusion Prevention System.</p> <p>Kontrola stron WWW.</p> <p>Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</p> <p>Zarządzanie pasmem (QoS, Traffic shaping).</p> <p>Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</p> <p>Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</p> <p>Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.</p>



Cyberbezpieczny Samorząd

	<p>Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.</p>
Polityki, Firewall	<p>Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <p>Translację jeden do jeden oraz jeden do wielu.</p> <p>Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</p> <p>W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</p> <p>Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <p>Amazon Web Services (AWS).</p> <p>Microsoft Azure</p> <p>Google Cloud Platform (GCP).</p> <p>OpenStack.</p> <p>VMware NSX.</p>
Połączenia VPN	<p>System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:</p> <p>Wsparcie dla IKE v1 oraz v2.</p> <p>Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).</p> <p>Obsługa protokołu Diffie-Hellman grup 19 i 20.</p> <p>Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</p> <p>Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</p> <p>Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</p> <p>Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</p> <p>Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.</p> <p>Mechanizm „Split tunneling” dla połączeń Client-to-Site.</p>



Cyberbezpieczny Samorząd

	<p>System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:</p> <p>Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.</p> <p>Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</p> <p>Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.</p>
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <p>Routingu statycznego.</p> <p>Policy Based Routingu.</p> <p>Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.</p>
Funkcje SD-WAN	<p>System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.</p>
Zarządzanie pasmem	<p>System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.</p> <p>System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
Ochrona przed malware	<p>Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR.</p> <p>System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania</p>



Cyberbezpieczny Samorząd

		<p>musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.</p> <p>System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p>
Ochrona atakami	przed	<p>Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.</p> <p>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p>
Kontrola aplikacji		<p>Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur</p>
Kontrola WWW		<p>Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p>



Cyberbezpieczny Samorząd

	<p>W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.</p> <p>Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.</p> <p>Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.</p>
Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:</p> <p>Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</p> <p>Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</p> <p>Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</p> <p>Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.</p> <p>Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.</p> <p>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
Zarządzanie	<p>Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</p>



Cyberbezpieczny Samorząd

	<p>System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.</p> <p>System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p>
Logowanie	<p>Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <p>W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.</p> <p>Musi istnieć możliwość logowania do serwera SYSLOG.</p>
Certyfikaty	<p>Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:</p> <p>ICSA lub EAL4 lub równoważne dla funkcji Firewall.</p>
Serwisy i licencje	<p>W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:</p> <p>Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres co najmniej do końca czerwca 2026 r.</p>
Gwarancja wsparcie	<p>Gwarancja: System musi być objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie</p>



Cyberbezpieczny Samorząd

	24x7.
Opisy do wymagań ogólnych	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.
Instalacja i konfiguracja	Konfiguracja UTM (przeniesienie konfiguracji z wykorzystywanego przez Zamawiającego urządzenia brzegowego; konfiguracja interfejsów, polityk dostępu, profili bezpieczeństwa, NAT, SSL VPN). Aktualizacja oprogramowania do najnowszej wersji zalecanej przez producenta sprzętu.

III. Zakup oraz konfiguracja serwera wirtualizacji wraz z systemem operacyjnym oraz licencjami do maszyn wirtualnych, licencji dostępowych. Usługa migracji systemów i wdrożenia wirtualizacji na serwerach.

	Wymagane minimalne parametry techniczne
Obudowa	Typu RACK, wysokość nie więcej niż 1U; Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym ułożenie kabli z tyłu serwera; Możliwość zainstalowania 8 dysków twardych hot plug 2,5"; Zainstalowane 4 szt. dysków SSD SATA 960GB, dyski skonfigurowane w RAID-5 podłączone do sprzętowego kontrolera RAID; Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.
Płyta główna	Dwuprocesorowa; Wyprodukowana i zaprojektowana przez producenta serwera; Możliwość instalacji procesorów 60-rdzeniowych; Zainstalowany moduł TPM 2.0;



Cyberbezpieczny Samorząd

	<p>4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5; Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH; 32 gniazda pamięci RAM; Obsługa 8 TB pamięci operacyjnej RAM DDR5; Wsparcie dla technologii: Memory Scrubbing; SDDC; ECC; Memory Mirroring; ADDDC; Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug. BIOS UEFI w specyfikacji 2.7.</p>
Procesory	<p>Dwa procesory 8-rdzeniowe, taktowanie bazowe 3,2 GHz, architektura x86_64; osiągające w teście SPEC CPU2017 Floating Point Rates wynik SPECrate2017_fp_base co najmniej 283 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta.</p>
Pamięć RAM	<p>64 GB pamięci RAM; DDR5 Registered 4800MT/s; Pamięci obsadzone modułami 16GB;</p>
Kontrolery LAN	<p>Interfejsy LAN: 4x 1Gbit Base-T; 2x10GBASE-T; 2x10Gb SFP+ (zamontowane 2 wkładki SFP+ Multi Mode Fiber 10GbE LC) Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;</p>
Kontrolery I/O	<p>Kontroler sprzętowy SAS/SATA RAID dla dysków wewnętrznych obsługujący poziomy RAID: 0, 1, 10, 5, 50;</p>
Porty	<p>Zintegrowana karta graficzna ze złączem VGA z tyłu serwera, dostępna</p>



Cyberbezpieczny Samorząd

	<p>opcja umożliwiająca uzyskania złącza VGA z przodu serwera;</p> <p>1 port USB 3.0 wewnętrzne;</p> <p>2 porty USB 3.0 dostępne z tyłu serwera;</p> <p>2 porty USB 3.0 na panelu przednim;</p> <p>Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;</p> <p>Ilość dostępnych złączy USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.</p>
Zasilanie, chłodzenie	<p>Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;</p> <p>Redundantne wentylatory hotplug</p>
Zarządzanie	<p>Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;</p> <p>informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:</p> <p>karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express;</p> <p>procesory CPU;</p> <p>pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;</p> <p>wbudowany na płycie głównej nośnik pamięci M.2 SSD;</p> <p>status karty zarządzającej serwerem;</p> <p>wentylatory;</p> <p>bateria podtrzymująca ustawienia BIOS płyty głównej;</p> <p>zasilacze;</p> <p>system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);</p> <p>Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:</p> <p>Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;</p> <p>Dedykowana karta LAN 1 Gb/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;</p>



Cyberbezpieczny Samorząd

	<p>Dostęp poprzez przeglądarkę Web, SSH;</p> <p>Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;</p> <p>Zarządzanie alarmami (zdarzenia poprzez SNMP);</p> <p>Możliwość przejęcia konsoli tekstowej;</p> <p>Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);</p> <p>Obsługa serwerów proxy (autentykacja);</p> <p>Obsługa VLAN;</p> <p>Możliwość konfiguracji parametru Max. Transmission Unit (MTU);</p> <p>Wsparcie dla protokołu SSDP;</p> <p>Obsługa protokołów TLS 1.2, SSL v3;</p> <p>Obsługa protokołu LDAP;</p> <p>Synchronizacja czasu poprzez protokół NTP;</p> <p>Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;</p> <p>Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, 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>Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;</p> <p>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>Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.</p>
Wspierane OS	<p>Microsoft Windows Server 2022, 2019;</p> <p>VMWare vSphere 8.0;;</p> <p>Suse Linux Enterprise Server 15;</p> <p>Red Hat Enterprise Linux 9, 8;</p> <p>Microsoft Hyper-V Server 2019</p>



Cyberbezpieczny Samorząd

Gwarancja	<p>Sprzęt musi być objęty gwarancją producenta w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub serwis lub wykonawcę. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;</p> <p>Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;</p> <p>Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;</p>
Dokumentacja, inne	<p>Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta na żądanie Zamawiającego;</p> <p>Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta na żądanie zamawiającego;</p> <p>Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterek;</p> <p>W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;</p> <p>Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;</p> <p>Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;</p> <p>Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04;</p> <p>Zgodność z normami: CB, RoHS, WEEE, GS oraz CE.</p>
Licencje	<p>Wraz z serwerem należy dostarczyć najnowsze wersje systemu operacyjnego</p> <p>Windows Serwer – licencje wieczyste, uwzględniającą ilość rdzeni serwerów i umożliwiające instalację nieograniczonej liczby maszyn wirtualnych z systemem Windows Serwer.</p>



Cyberbezpieczny Samorząd

	Licencje wieczyste typu na użytkownika CAL – 20 szt. Licencje wieczyste typu na użytkownika RDS CAL – 3 szt.
Instalacja i konfiguracja	<p>Instalacja serwerów w szafie RACK, podłączenia okablowania oraz niezbędnej konfiguracji serwera fizycznego (RAID, aktualizacja oraz konfiguracja wbudowanego oprogramowania zarządzającego).</p> <p>Instalacja i konfiguracja Hyper-V na serwerze fizycznym (konfiguracja sieci, przełączników wirtualnych, remote management, przestrzeni dyskowej na potrzeby maszyn wirtualnych).</p> <p>Instalacja i niezbędna konfiguracja czterech maszyn wirtualnych z systemem Windows Server 2022 (konfiguracja sieci, remote management, przestrzeni dyskowej, udziałów sieciowych DFS, DNS, DHCP, serwera wydruku).</p> <p>Migracja obecnych systemów zainstalowanych na serwerach fizycznych do wdrażanego środowiska wirtualnego.</p>

IV. Dostawa i instalacja serwera NAS wraz z systemem archiwizacji. Konfiguracja systemu archiwizacji danych.

	Wymagane minimalne parametry techniczne
Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark co najmniej 4580 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Dyski twarde	<p>8 dysków dedykowanych do oferowanego NAS, o parametrach: Typ dysku - HDD</p> <p>Format szerokości - 3,5" (LFF)</p> <p>Pojemność dysku - 6 TB</p> <p>Interfejs dysku - SATA III - 6 Gb/s</p> <p>Prędkość obrotowa - 5400 obr/min</p> <p>Bufor - 256 MB</p>
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 12 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu eSATA



Cyberbezpieczny Samorząd

Porty zewnętrzne	Minimum: 2 porty USB 3.2.1 1 eSATA (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) 2 porty 10Gb SFP+ (zamontowane 2 wkładki SFP+ Multi Mode Fiber 10Gbs LC)
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 1x 4-liniowe gniazdo x8
Wentylator obudowy	Min. 2 wentylatory 80 mm x 80 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	Maksymalny rozmiar pojedynczego wolumenu: 108 TB Minimalny liczba wewnętrznych wolumenów: 64 Minimalny liczba obiektów iSCSI Target: 128 Minimalny liczba jednostek iSCSI LUN: 256 Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	Minimalna liczba kont użytkowników: 2 048 Minimalna liczba grup użytkowników: 256 Minimalna liczba folderów współdzielonych: 512 Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 1000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń.



Cyberbezpieczny Samorząd

Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Oprogramowanie	<p>Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych</p> <p>Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów</p> <p>Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.</p>
Konserwacja	Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz
Gwarancja	Gwarancja musi obejmować urządzenie główne oraz dodatkowe akcesoria montażowe w postaci przesuwanych szyn rack



Cyberbezpieczny Samorząd

Instalacja i konfiguracja	Instalacja oraz konfiguracja oprogramowania do backupu (przygotowanie serwera NAS na potrzeby repozytorium kopii bezpieczeństwa, instalacja oprogramowania do wykonywania backupu, integracja systemu backupu z platformą wirtualizacyjną, przeprowadzenie testów odtworzeniowych).
---------------------------	---

V. Instalacja kontrolera domeny AD oraz wdrożenie domeny Microsoft Active Directory z migracją profili użytkowników.

Przedmiot zamówienia obejmuje wdrożenie usług katalogowych Microsoft Active Directory z wykorzystaniem maszyn wirtualnych z punktu 3 wraz z:

- utworzeniem niezbędnych jednostek organizacyjnych, użytkowników oraz polityk GPO (np. mapowanie udziałów sieciowych, modyfikacja ustawień przeglądarki internetowej, tworzenie skrótów na pulpitach użytkowników, automatyczna instalacja drukarek sieciowych na wybranych komputerach, automatyczna instalacja pakietów msi),
- konfiguracją zabezpieczeń dla środowiska stacji roboczych oraz systemów serwerowych,
- integracją urządzeń takich jak urządzenie ochrony brzegu, serwery NAS, drukarki sieciowe z domeną Active Directory
- dołączeniem komputerów do domeny włącznie z migracją profili użytkowników (maksymalnie 20 urządzeń).

Usługa ta powinna zawierać: analizę istniejącego środowiska, projekt, wdrożenie, dokumentację powykonawczą, asystę w rozwiązywaniu problemów "wieku dziecięcego".

VI. Zakup wraz z instalacją i konfiguracją zarządzalnego przełącznika sieciowego.

	Wymagane minimalne parametry techniczne
Ogólne	<ul style="list-style-type: none">• Typ i liczba portów - 48x 10/100/1000 RJ45, 4x 10Gigabit Ethernet SFP+• Obudowa 1U, rackmount (dostarczone uchwyty montażowe)• Możliwość stackowania przełączników – do 200 portów w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym Link Aggregation i port mirroring
Zarządzanie energią	Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az) Możliwość wyłączenia diod LED w celu oszczędzania energii
Parametry wydajnościowe	Przełącznik line-rate zapewniający pracę z pełną wydajnością wszystkich interfejsów Pamięć DRAM – 1GB



Cyberbezpieczny Samorząd

	<p>Pamięć Flash – 512MB</p> <p>Wielkość bufora pakietów – 1.5MB</p> <p>Obsługa 4000 sieci VLAN</p> <p>16.000 adresów MAC</p> <p>Wire-speed IPv4 routing – 990 tras statycznych; 128 interfejsów IP</p> <p>Obsługa ramek jumbo – do 9000 bajtów</p> <p>2000 IGMP group</p> <p>8 połączeń zagregowanych typu „port channel”</p> <p>Ilość wpisów w listach kontroli dostępu Security ACL – 1000</p>
Mechanizmy związane z bezpieczeństwem sieci	<p>Wiele poziomów dostępu administracyjnego poprzez konsolę</p> <p>Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN</p> <p>Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X</p> <p>Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC</p> <p>Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X</p> <p>Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard</p> <p>Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard</p> <p>Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+</p> <p>Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community</p> <p>Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priority, TCP flag. Obsługa czasowych list ACL</p> <p>Obsługa mechanizmów zapewniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC]</p> <p>Bezpieczny proces bootowania urządzenia</p> <p>Suplikant 802.1X - przełącznik można skonfigurować tak, aby działał jako suplikant do innego przełącznika</p>



Cyberbezpieczny Samorząd

<p>Mechanizmy związane z zapewnieniem jakości usług w sieci</p>	<p>Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi</p> <p>Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek</p> <p>Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)</p> <p>Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP</p> <p>Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi</p> <p>Kontrola szturmów dla ruchu broadcast/multicast/unicast</p> <p>Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP</p> <p>Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu</p>
<p>Inne</p>	<p>Obsługa protokołu SNTP</p> <p>Obsługa IGMPv1/2/3 i MLDv1/2 Snooping</p> <p>Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2</p> <p>Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:</p> <p>IEEE 802.1w Rapid Spanning Tree</p> <p>IEEE 802.1s Multi-Instance Spanning Tree</p> <p>Per-VLAN Rapid Spanning Tree (PVRST+)</p> <p>Obsługa 126 instancji protokołu STP</p> <p>Obsługa protokołu LLDP i LLDP-MED</p> <p>Obsługa Q-in-Q oraz Selective Q-in-Q</p> <p>Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad (LACP)</p> <p>Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego</p> <p>Możliwość uruchomienia funkcji serwera DHCP</p> <p>Przełącznik powinien umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN z możliwością konfiguracji do 4 sesji</p>



Cyberbezpieczny Samorząd

	<p>monitorujących</p> <p>Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)</p> <p>Obsługa protokołu sFlow</p> <p>Zasilacz AC 230V</p> <p>Praca w szerokim zakresie temperatur: -5oC – 50oC</p>
Zarządzanie	<p>Port konsoli – USB typu C i RJ45</p> <p>Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia</p> <p>Obsługa protokołów SNMPv3, SSHv2, https, syslog, SCP</p> <p>Aplikacja mobilna umożliwiająca łatwe zarządzania urządzeniami</p> <p>Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki</p> <p>Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu</p>
Instalacja i konfiguracja	<p>Konfiguracja dostarczonego przełącznika sieciowego oraz integracja z obecnie wykorzystywanym przełącznikiem Zamawiającego. Wdrożenie separacji sieci zgodnie z zatwierdzoną przez Zamawiającego koncepcją podziału sieci na podsieci (VLAN).</p>

VII. Zakup zasilaczy awaryjnych UPS do stacji roboczych – 10 szt.

Poniżej wyspecyfikowano wymagania minimalne dla 1 szt. UPS do stacji roboczych. Zamawiający oczekuje dostawy 10 szt. UPS spełniających poniższe, minimalne wymagania:

	Wymagane minimalne parametry techniczne
Moc pozorna	500 VA
Moc czynna	300 W
Architektura UPS-a	line-interactive
Liczba faz na wejściu	1 (230V)
Liczba	1



Cyberbezpieczny Samorząd

akumulatorów	
Napięcie	12 V
Pojemność akumulatora	7 Ah
Czas przełączenia (maks.)	10 ms
Czas ładowania	8 h
Typ obudowy	Tower
Funkcje specjalne	AVR
Porty zasilania we.	IEC-C14
Porty zasilania wy.	3 x IEC-C13
Gniazda we/wy	1 x USB (Type B) 2 x RJ-45 LAN
Gwarancja	TAK
Wymagania środowiskowe	Temperatura otoczenia dla pracy urządzenia: 0-40 °C Wilgotność względna: 0-95 % Temperatura otoczenia dla przechowywania: -15-40 °C Wilgotność względna (przechowywanie): 0-95 %

VIII. Zakup zasilaczy awaryjnych UPS do serwerów – 2 szt.

Poniżej wyspecyfikowano wymagania minimalne dla 1 szt. UPS do serwerów. Zamawiający oczekuje dostawy 2 szt. UPS spełniających poniższe, minimalne wymagania:

	Wymagane minimalne parametry techniczne
Moc pozorna	Min. 3000VA
Moc czynna	Min. 2700W
Architektura UPS-a	on-line podwójna konwersja
Zakres napięcia wejściowego przy pełnym obciążeniu	175 – 280V
Poziom zniekształceń THDu	Mniejsze niż 2%



Cyberbezpieczny Samorząd

Ilość gniazd wyjściowych	IEC C13 x 6; IEC C19 x 1
Sprawność	do 94%
Czas podtrzymania dla obciążenia 50% mocą czynną	Minimum 12 min.
Poziom hałasu	Poniżej 46 dB
Interfejsy komunikacyjne	SMART Slot x 1, RS-232 Port x 1, USB Port x 1, REPO x 1
Wyświetlacz	Wyświetlacz LCD i diody LED
Możliwość wymiany baterii pod napięciem	Tak „hot swap”
Możliwość zastosowania modułu bypass-u serwisowego zewnętrznego	Bypass serwisowy zapewniający komunikację z UPSem oraz dystrybucją IEC C13 x 6; IEC C19 x 1.
Możliwość rozbudowy o dodatkowy moduł bateryjny	Tak
Gwarancja	Tak

OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI II:

1. Zakup agregatu prądotwórczego wraz z montażem

Dane techniczne agregatu prądotwórczego

Agregat prądotwórczy ma spełniać wymagania ISO8528 lub normy równoważnej i powinien być wyprodukowany zgodnie ze standardami ISO 9001 lub normy równoważnej oraz posiadać znak CE.

Układy elektryczne agregatu prądotwórczego powinny być zgodnie z EN 60950, EN 61000-6-2, EN 61000-6-2, EN 61000-6-4 lub normami równoważnymi.

Dane agregatu prądotwórczego:



Cyberbezpieczny Samorząd

- napięcie – 400.230 V;
- częstotliwość – 50 Hz;
- współczynnik mocy $\cos \phi$ - 0,8;
- moc awaryjna ESP – 20 kVA / 16 kW (zgodnie z ISO 8528);
- moc znamionowa PRP – 18 kVA / 14,4 kW (zgodnie z ISO 8528);
- prąd – 25,98 A.

Tryb rezerwowy: praca ciągła przy zmiennym obciążeniu na czas awarii sieci zasadniczej. Nie dopuszcza się przeciążeń. Zgodnie z normą ISO8528 lub równoważną. Tryb ciągły: praca ciągła przy zmiennym obciążeniu przez czas nieograniczony z możliwością przeciążania o 10% przez 1 godzinę na każde 12 godzin pracy. Zgodnie z ISO8528, ISO3046 lub równoważną.

Specyfikacja standardowa

SILNIK:

- wysokoprężny, przemysłowy silnik;
- czterosuwowy, chłodzony cieczą, turbodoładowany;
- elektroniczny regulator obrotów;
- bezpośredni system wtrysku paliwa;
- wymienne filtry paliwa, oleju i powietrza;
- akumulatory rozruchowe kwasowe mocowane na agregacie i okablowanie;
- chłodnica z układem wentylatorów;
- elastyczne przyłącze paliwowe oraz ręczna pompa do opróżniania miski olejowej;
- tłumik wydechu standardu przemysłowego z przyłączem elastycznym;
- ogrzewacz płaszcza wodnego (w agregatach z automatyką rozruchu);
- buforowa ładowarka akumulatorów.

PRĄDNIKA:

- bezszczotkowa, jednołożyskowa;
- klasa izolacji h;
- standardowy stopień ochrony: IP23;
- samowzbudna, samoregulująca;
- uzwojenia przystosowane do pracy w tropikach (pokryte lakierem epoksydowym);
- półprzewodnikowy, automatyczny regulator napięcia.

RAMA:

- Kompletny zespół prądotwórczy jest zmontowany jako jedna całość i osadzony na stalowej poprzec poduszki antywibracyjne;
- z ramą agregatu zintegrowany jest zbiornik paliwa;



Cyberbezpieczny Samorząd

- zespół prądotwórczy może być podnoszony lub delikatnie przesuwany za ramę;
- obrotowy wskaźnik poziomu paliwa oraz spust paliwa na zbiorniku;
- oka do unoszenia za pomocą dźwigu.

OBUDOWA (OPCJONALNIE):

- konstrukcja modułowa lub kontenerowa;
- drzwi dostępne z każdej strony;
- wszystkie elementy stalowe lakierowane proszkowo;
- tłumik wydechowy stalowy zabezpieczony przed wpływem warunków atmosferycznych;
- rura wydechowa izolowana termicznie;
- przycisk wyłącznika awaryjnego zainstalowany na zewnątrz obudowy.

System sterowania i nadzoru

Szafa sterowania i nadzoru pracy agregatu zainstalowana na ramie agregatu.

Wypożyczenie szafy powinno obejmować:

1. Panel sterowania, nadzoru pracy agregatu, kontroli obecności sieci i automatycznego rozruchu wyposażony w:

- elektroniczny moduł kontroli i sterowania ARK700E (opcjonalne sterowniki – Comap, Deep Sea do pracy wyspowej lub synchronicznej z siecią;
- prostownik ładowania akumulatorów;
- przycisk wyłącznika awaryjnego (p/poż).

a) WŁAŚCIWOŚCI MODUŁU STEROWANIA

- moduł do monitorowania sieci przemysłowej i automatycznego uruchomienia i zatrzymania agregatu;
- moduł oparty o technologie mikroprocesorową;
- automatyczna kontrola i sterowanie aparatami sieci i agregatu w panelu przełączania źródła zasilania – SZR;
- kontrola parametrów mechanicznych silnika i elektrycznych generatora;
- sygnalizacja alarmów przy użyciu diod LED i na wyświetlaczu LCD;
- rejestracja zdarzeń (do 50 zdarzeń np. wyłączeń, alarmów itp);
- prosta obsługa za pomocą przycisków sterujących i wyświetlacza LCD z czytelnym menu;
- kompletne trójfazowy nadzór sieci i agregatu (zbyt niskie napięcie, przepięcie, asymetria fazy, nieprawidłowa kolejność faz, niedoczęstotliwość i nadmierna częstotliwość);
- teksty w 7 językach: włoski, angielski, francuski, niemiecki, hiszpański, portugalski i język programowalny;
- połączenie magistrali CAN SAEJ1939;
- port szeregowy RS232, RS485 i USB;



Cyberbezpieczny Samorząd

- protokół MOD Bus RTU;
- możliwość uruchomienia generatora, gdy poziom naładowania akumulatora jest niski;
- zarządzanie tankowaniem ze zbiornika roboczego ze zbiornika magazynowego;
- zegar do programowania uruchamiania lub zatrzymywania agregatu;
- automatyczny test.

b) REALIZOWANE POMIARY (ODCZYT NA WYŚWIETLACZU LCD)

- napięcie prądnicy [V] F-F, F-N;
- prąd pobierany z prądnicy [A] (L1,L2,L3);
- częstotliwość prądnicy [Hz];
- parametry prądnicy kW, cos f, kVAr, kWh, kVAh, kVArh;
- godziny pracy [h];
- obroty silnika;
- ciśnienie oleju silnikowego [Bar];
- temperatura silnika [°C];
- napięcie sieci [V] F-F, F-N;
- częstotliwość sieci [Hz];
- napięcie akumulatorów [V DC].

OSTRZEŻENIA (Nie skutkują wyłączeniem silnika): uszkodzona ładowarka akumulatorów, niskie napięcie akumulatorów, błąd zatrzymania silnika, chwilowe przeciążenie, niski poziom paliwa (opcja).

ALARMY OSTRZEGAWCZE (Skutkują wyłączeniem silnika, gdy ALARM OSTRZEGAWCZY wyświetla się przez dłuższy czas (czas zaprogramowany w kontrolerze)): niskie ciśnienie oleju, wysoka temperatura silnika, niska temperatura silnika, zbyt wysokie/niskie obroty silnika/częstotliwość, zbyt wysokie/niskie napięcie prądnicy, błąd jednostki ECU (komputera) silnika.

ALARMY KRYTYCZNE (Skutkują natychmiastowym wyłączeniem silnika) W niektórych sytuacjach wcześniej wyświetla się ALARM OSTRZEGAWCZY.

2. Wyłącznik główny generatora z zabezpieczeniami przeciwzwarciovymi i przeciążeniowymi oraz przyłączem kablowym – opcjonalnie dostępne inne typy wyłącznika.

PARAMETRY TECHNICZNE SILNIKA SPALINOWEGO - minimalne		
Liczba i układ cylindrów		4 cylindrów
Doładowanie i chłodzenie powietrza dolotowego		Turbosprężarka + chłodnica powietrza
Moc netto PRP	kW	18
Pojemność całkowita	L	2,3
Obroty znamionowe	obr/min	1500



Cyberbezpieczny Samorząd

Regulator obrotów		Elektroniczny	
Pojemność układu smarowania (olej)	L	11	
Całkowity przepływ chłodzenia	L	13,3	
Całkowity przepływ powietrza	m ³ /min	1,38	
Przepływ powietrza chłodzącego	m ³ /min	63	
Przepływ spalin	m ³ /min	4,3	
Temperatura spalin	Co	≤700	
Napięcie układu rozruchowego	V DC	12V	
Moc rozrusznika	kW	3	
Prąd ładowania akumulatora	A	55	
Standardowa pojemność baterii		1 x 60Ah	
Zużycie paliwa	Obciążenie	100%	75%
	L/h	4,7	3,6

PARAMETRY TECHNICZNE PRĄDNICY - minimalne		
Częstotliwość	Hz	50
Moc	kVA	18,8
Konstrukcja		bezszcotkowa
Współczynnik mocy cosφ		0.8
Ilość faz		3
Napięcie	V	400/230
Stopień ochrony		IP23
Klasa izolacji		H
Regulator napięcia (AVR)		Elektroniczny

WYMIARY I CIĘŻAR - maksymalne					
Wersja otwarta	Ciężar agregatu suchego	Długość	Szerokość	Wysokość	Pojemność zbiornika paliwa
	kg	mm	mm	mm	L
	550	1530	900	1120	60



Cyberbezpieczny Samorząd

Wersja w obudowie dźwiękochłonnej odpornej na warunki atmosferyczne	Ciężar agregatu suchego	Długość	Szerokość	Wysokość	Pojemność zbiornika paliwa
	kg	mm	mm	mm	L
	660	2055	960	1244	60

Wypożyczenie opcjonalne

SILNIK

- podgrzewacz oleju;
- chłodzenie wyniesioną chłodnicą.

PRĄDNICA

- układ antykondensacyjny;
- wzбудnica PMG z regulatorem napięcia;
- 3-biegunowy wyłącznik główny.

PANEL KONTROLI

- panel zdalnej sygnalizacji pracy agregatu;
- bezpotencjałowe styki alarmowe;
- kontrola doziemienia.

INNE

- magazynowy zbiornik paliwa;
- ręczna pompa spustu oleju;
- alarm niskiego poziomu paliwa;
- podwozia jezdne;
- kontener;
- przepływomierz.