



Zamówienie – kompleksowe i całościowe dostarczenie rozwiązania IT w celu polepszenia cyberbezpieczeństwa.

W ramach tego rozwiązania dostarczone zostanie rozwiązanie IT w postaci systemów zabezpieczeń danych, zarządzalnych urządzeń sieciowych, serwera fizycznego, macierzy dyskowej, a także zestawu zasilania awaryjnego.

Celem zamówienia jest zwiększenie poziomu cyberbezpieczeństwa ww. podmiotów poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych. Celem jest wdrożenia mechanizmów i środków zwiększających 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.

#### **Przedmiot obejmuje kompleksowe rozwiązanie:**

- I. Serwer backup;
- II. Bibliotekę taśmową;
- III. Macierz dyskową;
- IV. Kartę sieciową dwuportową – 2 szt.;
- V. Oprogramowanie do backupu;
- VI. System firewall;
- VII. Przełącznik sieciowy;
- VIII. Zasilacz awaryjny typ. 1 – 18 szt.
- IX. Zasilacz awaryjny typ 2 z dodatkowym modulem baterijnym wraz z oprogramowaniem zarządzającym;
- X. Agregat prądotwórczy

Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:

1. Wykonanie Projektu Technicznego dostarczanej infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:



## Cyberbezpieczny Samorząd

- dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
- nazwy oraz szczegółowa adresacja poszczególnych elementów,
- planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca, zaprojektowanie kompleksowego systemu ochrony danych opartego na funkcjach macierzy oraz oprogramowania standardowego z uwzględnieniem specyfiki całego projektu,
- wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
- harmonogram prac.

Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

2. Instalacja oraz konfiguracji oprogramowania zgodnie z wytycznymi Zamawiającego (m.in. wirtualizacja, instalacja systemu backup na serwerze, skonfigurowanie zadań backup na dyski lokalne serwera oraz na taśmy) Instalacja i konfiguracja systemu firewall, oraz przełącznika (m.in. segmentacja sieci (VLAN), reguły dostępu, do Internetu oraz komunikacji wewnętrznej, stworzenie przykładowych polityk zezwalających na ruch pomiędzy segmentami, konfiguracja funkcjonalności L2 oraz L3, Remote Access VPN, SSL VPN, integracja z AD) Testy rozwiązania.
3. Instrukcja dla administratorów demonstrujący sposób zarządzania środowiskiem.
4. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:
  - specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
  - końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
  - konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
  - komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,
  - dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim,
  - szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury Zamawiającego, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej,
  - zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni,
  - po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępne do kont „super użytkowników”.

Wymagania w zakresie instalacji i konfiguracji:

1. Montaż urządzeń w posiadanej szafie rack 42U w pomieszczeniu udostępnionym przez Zamawiającego.
2. Okablowanie urządzeń dla komunikacji LAN
3. Okablowanie urządzeń dla komunikacji SAN, instalacja kart w serwerach dla komunikacji iSCSI



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA



## Cyberbezpieczny Samorząd

4. Podłączenie urządzeń do listew zasilających PDU.
5. Aktualizacja oprogramowania układowego wszystkich komponentów.
6. Podłączenie do sieci LAN (rekonfiguracja przełączników)
7. Instalacja agregatu prądotwórczego we wskazanym miejscu przez zamawiającego oraz podłączenie do istniejącej sieci elektrycznej wraz z konfiguracją.

Wykonawca po zainstalowaniu i skonfigurowaniu sprzętu i oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania dostarczonego sprzętu oraz oprogramowania.

### **UWAGA**

Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie przedmiotu zamówienia, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego.

Zamieszczone w specyfikacji nazwy technologicznych lub producentów kluczowych komponentów użyto jedynie w celu przykładowym.

Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w opisie przedmiotu zamówienia mogą być zastąpione urządzeniami bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie przedmiotu zamówienia. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w niniejszym zaproszeniu, ani do zmiany ceny.

### **I. Serwer backup – 1 szt.**

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3,5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiającym montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.  Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprosesorowych
Procesor	Zainstalowany jeden procesor, min. 16-rdzeniowy, min. 3.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiającym osiągnięcie wyniku min. 177 w teście SPECrate2017_int_base w konfiguracji jedno procesorowej,



## Cyberbezpieczny Samorząd

	dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> . Możliwość obsługi procesorów 128 rdzeniowych
<b>RAM</b>	Minimum 64GB DDR5 RDIMM 4800MT/s, na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do min. 3TB pamięci RAM.
<b>Zabezpieczenia pamięci RAM</b>	Patrol Scrubbing
<b>Gniazda PCI</b>	Minimum 8 slotów PCIe
<b>Interfejsy sieciowe/FC/SAS</b>	Min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 Interfejsy SFP28 muszą być wyposażone we wkładki 10Gb SFP+ MM. Dostarczenie 2 światłowodów MM OM3 LC-LC o długości minimum 3m. Dodatkowa, zewnętrzna, czteroportowa karta 12Gb SAS HBA.
<b>Dyski twarde</b>	Zainstalowane: <ul style="list-style-type: none"><li>• 6 dysków SAS o pojemności min. 8TB, 12Gbps, Hot-Plug.</li><li>• 2 dyski SSD SATA RI o pojemności min. 480GB 6Gbps, Hot-Plug.</li></ul> Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 480GB/960GB Hot-Plug z możliwością konfiguracji RAID 1.
<b>Kontroler RAID</b>	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60
<b>Wbudowane porty</b>	3x USB w tym przynajmniej 1x USB 3.0 1x port VGA na przednim panelu obudowy Możliwość rozbudowy o port RS232
<b>Video</b>	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1920x1080
<b>System operacyjny / dodatkowe oprogramowanie</b>	Windows Server 2022 Standard na odpowiadającą CPU liczbę rdzeni.
<b>Wentylatory</b>	Redundantne
<b>Zasilacze</b>	Redundantne, Hot-Plug min. 700W każdy wraz z kablami zasilającymi o długości min. 2m.
<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"><li>• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech.</li><li>• Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li><li>• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li><li>• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li></ul>



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>• Moduł TPM 2.0</li><li>• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</li><li>• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li></ul>
<b>Karta Zarządzania</b>	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:</p> <ul style="list-style-type: none"><li>• zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li><li>• zdalne monitorowanie i informowanie o statusie serwera (np. prędkości obrotowej wentylatorów, konfiguracji serwera);</li><li>• szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li><li>• możliwość podmontowania zdalnych wirtualnych napędów;</li><li>• wirtualną konsolę z dostępem do myszy, klawiatury;</li><li>• wsparcie dla Ipv6;</li><li>• wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li><li>• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li><li>• możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</li><li>• integracja z Active Directory;</li><li>• możliwość obsługi przez dwóch administratorów jednocześnie;</li><li>• wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li><li>• możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li><li>• możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li></ul>
<b>Certyfikaty</b>	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważnymi</p> <p>Serwer musi posiadać deklaracja CE.</p>
<b>Dokumentacja użytkownika</b>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
<b>Warunki gwarancji</b>	<p>Minimum 24-miesięczna gwarancja producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</p> <p>Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</p>





## Cyberbezpieczny Samorząd

Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.

Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.

### II. Biblioteka taśmowa – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do zamontowania w szafie rack, wbudowany czytnik kodów kreskowych wraz z kablem zasilającym.
Napęd	1x LTO9
Interfejs	SAS 12Gb/s
Liczba slotów	10 w tym 1 slot we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów W komplecie min.: <ul style="list-style-type: none"><li>• 1 taśma czyszcząca</li><li>• 10 taśm LTO9</li><li>• Etykiety do taśm LTO9 o numerach 1-200</li><li>• Kabel SAS 12Gb 2m</li></ul>
Dodatkowe	<ul style="list-style-type: none"><li>• interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD</li><li>• wyjmowany magazynek</li><li>• wsparcie dla nośników LTO WORM (Write Once, Read Many)</li><li>• Obsługa SNMP, TLS1.2 oraz IP6</li></ul>
Warunki gwarancji dla autoloadera	Gwarancja producenta realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).





## Cyberbezpieczny Samorząd

### III. Macierz dyskowa – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do instalacji w standardowej szafie RACK 19", macierz musi zajmować maksymalnie 2U i pozwalać na instalację 24 dysków 2.5".
Kontrolery	Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów 25Gb iSCSI w standardzie SFP28
Kable/wkładki	4 kable, SFP28 to SFP28, 25GbE, Passive Copper Twinax Direct Attach Cable, 3 metry
Cache	16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, przechowywana przez min. 72h w razie awarii.
Dyski	Zainstalowane: 6 dysków 2.4TB 10K SAS 12Gbps  Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
Oprogramowanie/Funkcjonalności	Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5.  Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN'ów oraz 1024 kopii migawkowych na całą macierz.  Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między różnymi typami dysków.  Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 8TB poprzez dyski SSD.  Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji.  Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym.
Wsparcie dla systemów operacyjnych	Windows Server 2022, Windows Server 2019, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, VMware ESXi, Citrix XenServer



## Cyberbezpieczny Samorząd

<b>Bezpieczeństwo</b>	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
<b>Warunki gwarancji dla macierzy</b>	<p>Gwarancja realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.</p> <p>Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.</p> <p>Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.</p> <p>W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).</p>
<b>Dokumentacja użytkownika</b>	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
<b>Certyfikaty</b>	Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2015 lub równoważną.

#### IV. Karta sieciowa dwuportowa – 2 szt.

Karta 2-portowa 10/25GbE low-profile do posiadanych serwerów.

#### V. Oprogramowanie do backupu

##### Wymagania minimalne

Licencja wieczysta na 10 maszyn wirtualnych. Wsparcie producenta przez okres co najmniej 24 miesiące, 24/7. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.

Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.

Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.





## Cyberbezpieczny Samorząd

### Wymagania minimalne

Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

Oprogramowanie musi wspierać niezmiennosć kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.

Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).

Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.

Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.

Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.

Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji.

Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.

Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.

Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.

Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastora.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.

Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.

Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).

Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA



## Cyberbezpieczny Samorząd

### Wymagania minimalne

Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.

Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.

Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).

Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.

Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchamianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.

Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.

Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny



## Cyberbezpieczny Samorząd

### Wymagania minimalne

obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem

Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

### VI. System Firewall – 1 szt.

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Wymagania Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były 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.



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA



## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<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 3 administratorów do poszczególnych instancji systemu.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"><li>• Firewall.</li><li>• Ochrony w warstwie aplikacji.</li><li>• Protokołów routingu dynamicznego.</li></ul>
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"><li>1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.</li><li>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</li><li>3. Monitoring stanu realizowanych połączeń VPN.</li><li>4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.</li></ol>
Interfejsy, Dysk, Zasilanie:	<ol style="list-style-type: none"><li>1. System realizujący funkcję Firewall musi dysponować minimum:<ul style="list-style-type: none"><li>• 10 portami Gigabit Ethernet RJ-45.</li></ul></li><li>2. System Firewall musi posiadać wbudowany port konsoli szeregowy oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li><li>3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.</li><li>4. System musi być wyposażony w zasilanie AC.</li></ol>
Parametry wydajnościowe:	<ol style="list-style-type: none"><li>1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.</li><li>2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.</li><li>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.</li><li>4. Wydajność szyfrowania IPSec VPN nie mniej niż 6.2 Gbps.</li><li>5. 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.</li><li>6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.</li><li>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej</li></ol>







## Cyberbezpieczny Samorząd

PARAMETR		CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
		SSL dla ruchu http – minimum 620 Mbps.
Funkcje Bezpieczeństwa:	Systemu	<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> <ol style="list-style-type: none"><li>1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</li><li>2. Kontrola Aplikacji.</li><li>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.</li><li>4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.</li><li>5. Ochrona przed atakami - Intrusion Prevention System.</li><li>6. Kontrola stron WWW.</li><li>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</li><li>8. Zarządzanie pasmem (QoS, Traffic shaping).</li><li>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</li><li>10. 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.</li><li>11. Analiza ruchu szyfrowanego protokołem SSL.</li></ol>
Polityki, Firewall		<ol style="list-style-type: none"><li>1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</li><li>2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<ul style="list-style-type: none"><li>• Translację jeden do jeden oraz jeden do wielu.</li><li>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</li></ul></li><li>3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</li><li>4. 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.<ul style="list-style-type: none"><li>• Amazon Web Services (AWS).</li><li>• Microsoft Azure</li><li>• Cisco ACI.</li><li>• Google Cloud Platform (GCP).</li><li>• OpenStack.</li><li>• VMware vCenter (ESXi).</li></ul></li></ol>
Połączenia VPN		<ol style="list-style-type: none"><li>1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:<ul style="list-style-type: none"><li>• Wsparcie dla IKE v1 oraz v2.</li><li>• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).</li></ul></li></ol>



## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<ul style="list-style-type: none"><li>• Obsługa protokołu Diffie-Hellman grup 19 i 20.</li><li>• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.</li><li>• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</li><li>• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li><li>• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</li><li>• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.</li><li>• Mechanizm „Split tunneling” dla połączeń Client-to-Site.</li></ul> <p>2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</li><li>• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.</li></ul>
Routing i obsługa łączy WAN	<p>1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <ul style="list-style-type: none"><li>• Routingu statycznego.</li><li>• Policy Based Routingu.</li><li>• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.</li></ul>
Zarządzanie pasmem	<p>1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.</p> <p>3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
Ochrona przed malware	<p>1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.</p> <p>3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z</p>







## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>usługi typu Sandbox w chmurze.</p> <p>5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p>
Ochrona przed atakami	<ol style="list-style-type: none"><li>1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</li><li>2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.</li><li>3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li><li>4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.</li><li>5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</li><li>6. 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.</li><li>7. Wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet.</li></ol>
Kontrola aplikacji	<ol style="list-style-type: none"><li>1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</li><li>2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li><li>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</li><li>4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</li><li>5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.</li></ol>
Kontrola WWW	<ol style="list-style-type: none"><li>1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</li><li>2. 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.</li><li>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.</li><li>4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</li><li>5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.</li></ol>





## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<ol style="list-style-type: none"><li>6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.</li><li>7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.</li></ol>
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"><li>1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:<ul style="list-style-type: none"><li>• Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li><li>• Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li><li>• Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li></ul></li><li>2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.</li><li>3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.</li></ol>
Zarządzanie	<ol style="list-style-type: none"><li>1. 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.</li><li>2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.</li><li>3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</li><li>4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.</li><li>5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</li><li>6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</li><li>7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</li></ol>
Logowanie	<ol style="list-style-type: none"><li>1. 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.</li></ol>



## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<ol style="list-style-type: none"><li>2. 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.</li><li>3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.</li><li>4. Musi istnieć możliwość logowania do serwera SYSLOG.</li></ol>
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: <ul style="list-style-type: none"><li>• ICSA lub EAL4 dla funkcji Firewall lub równoważne.</li></ul>
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 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 do końca czerwca 2026 r.
Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, 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 24x7.

### VII. Przełącznik sieciowy – 1 szt.

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Wymagania Ogólne	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z rozwiązaniem UTM wymagany w niniejszym postępowaniu
Parametry fizyczne platformy	Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V. Wbudowany redundantny zasilacz. Maksymalny pobór mocy: 50 W. Minimalny zakres temperatury pracy: 0-50°C.
Interfejsy sieciowe wymagania minimalne	<ol style="list-style-type: none"><li>1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w</li></ol>



## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	ilości: a) 48 porty GE RJ-45. b) 4 porty 10 GE SFP+.
Zarządzanie	<ol style="list-style-type: none"><li>1. Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.</li><li>2. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.</li><li>3. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li><li>4. Wsparcie dla SNMP w wersjach 1-3</li><li>5. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li><li>6. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li><li>7. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li><li>8. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li><li>9. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li><li>10. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li><li>11. Automatycznie wykonywane rewizje konfiguracji.</li></ol>
Parametry wydajnościowe	<ol style="list-style-type: none"><li>1. Przepustowość urządzenia - min. 176 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps.</li><li>2. Tablica adresów MAC o pojemności co najmniej 32 k wpisów.</li><li>3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.</li></ol>
Wymagane funkcje	<ol style="list-style-type: none"><li>1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li><li>2. Obsługa Jumbo Frames.</li><li>3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li><li>4. Agregacja portów zgodna ze standardem 802.3ad.</li><li>5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li><li>6. Wsparcie dla Private VLAN.</li><li>7. Obsługa routingu statycznego.</li><li>8. Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.</li><li>9. Port-mirroring.</li><li>10. Uwierzytelnianie 802.1x na poziomie portu.</li><li>11. Uwierzytelnianie 802.1x w oparciu o adres MAC.</li><li>12. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li><li>13. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li><li>14. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li><li>15. Obsługa protokołu sFlow.</li></ol>





## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
<b>Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC</b>	<ol style="list-style-type: none"><li>1. Przełączniki 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). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:</li><li>2. Centralne zarządzanie konfiguracją urządzenia</li><li>3. Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li><li>4. Centralne zarządzanie sieciami VLAN.</li><li>5. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u</li><li>6. Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..</li><li>7. Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li><li>8. Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.</li><li>9. Automatyczna detekcja i rekomendacje konfiguracji.</li><li>10. Przesyłanie logów na zewnętrzny serwer syslog.</li><li>11. Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.</li><li>12. Obsługa białych i czarnych list adresów MAC.</li><li>13. Wykrywanie aplikacji komunikujących się w sieci.</li><li>14. Musi być możliwe redundantne połączenie z elementami zarządzającymi.</li><li>15. 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.</li></ol>
<b>Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa</b>	<ol style="list-style-type: none"><li>1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.</li><li>2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li></ol>
<b>Gwarancja oraz wsparcie</b>	<ol style="list-style-type: none"><li>1. System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesiące, 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 24x7.</li></ol>
<b>Opisy do wymagań ogólnych</b>	<ol style="list-style-type: none"><li>1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć (na każde żądanie Zamawiającego) dokument pochodzący od importera tej</li></ol>





## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	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.

### VIII. Zasilacz awaryjny typ I – 18 szt.

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Moc (VA / W)	1600 VA / 900 W
Typ obudowy	Wieżowa (Tower)
Technologia	Line-Interactive
Układ automatycznej regulacji napięcia (AVR)	Tak
Napięcie znamionowe wejściowe	220 – 240 V
Zakres napięcia wejściowego bez użycia akumulatora	140 – 300 V
Napięcie wyjściowe	230 V (regulowane 220/230/240 V)
Zakres częstotliwości wyjściowej	50 / 60 Hz (46 - 65 Hz zakres roboczy)
Czas przełączania	Maks. 10 ms dla przejścia z trybu normalnego do trybu bateryjnego
Sprawność	Min. 94% (przy pracy normalnej)
Przewód zasilający	Stały przewód z wtykiem CEE 7/7 (Unischuko)
Gniazda wyjścia	4x gniazda typu E (polskie z bolcem)
Czas podtrzymania dla obciążenia 500W	Min. 4 minut
Czas podtrzymania dla obciążenia 270W	Min. 12 minut
Zimny start	Tak
Automatyczny test baterii	Tak, automatyczny test baterii i alarm konieczności wymiany baterii
Port komunikacyjny	Tak, USB
Funkcja Auto-	Tak, umożliwiająca automatyczne ponowne uruchomienie, gdy zasilanie





## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
restartu	sieciowe powróci po całkowitym rozładowaniu baterii.
Zarządzanie zasilaczem	Automatyczne połączenie z narzędziami zasilania w systemie Windows w celu bezpiecznego wyłączenia systemu.
Oprogramowanie dostarczone z UPS (lub dostępne do pobrania na stronie internetowej producenta)	<p>Wymagane cechy oprogramowania:</p> <ul style="list-style-type: none"><li>• Bezpieczne zamykanie systemów operacyjnych,</li><li>• Dostęp do statusu pracy UPS i dziennika zdarzeń,</li><li>• Analiza zużycia i kosztów energii,</li><li>• Konfiguracja parametrów zasilacza UPS,</li><li>• Automatyczne aktualizacje programu.</li></ul> <p>Oprogramowanie kompatybilne z systemem Windows 10/11.</p>
Stopień ochrony	IP20
Poziom hałasu	<ul style="list-style-type: none"><li>• Przy pracy z sieci maks. 25 dBA</li><li>• Przy pracy z baterii lub w trybie AVR maks. 40 dBA</li></ul>
Certyfikaty i zgodność z normami	IEC/EN 62040-1; IEC/EN 62040-2, IEC/EN 62040-3; CE lub równoważne
Gwarancja	Gwarancja producenta min. 24 miesiące

### IX. Zasilacz awaryjny typ II z dodatkowym modułem bateryjnym – 1 szt.

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Moc pozorna	3000 VA
Moc rzeczywista	3000 W
Współczynnik mocy	1
Topologia (klasyfikacja IEC 62040-3)	Line-interactive (czysta sinusoida, AVR)
Typ obudowy UPS	Uniwersalna Tower/Rack maks. 2U
Liczba, typ gniazd wyjściowych, możliwość sterowania	<p>8x IEC C13 (10A), 2x IEC C19 (16A), W tym 2 grupy gniazd z możliwością sterowania:</p> <ol style="list-style-type: none"><li>1. 2x IEC C13</li><li>2. 2x IEC C13 + 1x IEC C19</li></ol>
Typ gniazda wejściowego	Gniazdo IEC C20 (16A)
Czas podtrzymania	<ul style="list-style-type: none"><li>• 20 minut dla obciążenia 3000W,</li><li>• 40 minut dla obciążenia 1500W,</li><li>• możliwość wydłużenia czasu podtrzymania do 75 minut dla obciążenia 3000W poprzez dołożenie kolejnych modułów bateryjnych</li></ul>
Napięcie znamionowe	230 V
Tolerancja napięcia prostownika	160 - 294 V



## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Częstotliwość znamionowa	50/60 Hz autodetekcja
Tolerancja częstotliwości	47 - 70 Hz (system 50 Hz) / 57 do 70 Hz (system 60 Hz)
Napięcie znamionowe wyjściowe	230 V (domyślnie) / 208/220/240 V
Częstotliwość wyjściowa	50/60 Hz
Baterie wymieniane przez użytkownika "na gorąco"	Tak
Ochrona przed przeładowaniem	Tak
Ochrona przed głębokim rozładowaniem	Tak
Okresowy automatyczny test baterii	Tak
Zimny start	Tak
System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
Interfejs komunikacyjny	<ul style="list-style-type: none"><li>• USB i RS232</li><li>• karta Web/SNMP</li><li>• złącze dla zdalnego awaryjnego wyłączenia</li><li>• złącze dla zdalnego załączenia/wyłączenia</li><li>• złącze dla wyjściowego styku przekaźnikowego</li></ul>
Panel sterowania z wyświetlaczem LCD	<ul style="list-style-type: none"><li>• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS-a) ze wskazaniem chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh)</li><li>• Poziomy rząd przycisków sterowania</li><li>• Poziomy rząd wskaźników stanu: trybu normalnego (zielony), trybu bateryjnego (żółty), usterki (czerwony)</li><li>• Pasek LED sygnalizujący stan pracy</li><li>• Sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie)</li></ul>



## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Przyciski sterujące	<ul style="list-style-type: none"><li>• przycisk Escape (anulowanie)</li><li>• przyciski funkcyjne (przewijanie w górę i w dół)</li><li>• przycisk Enter (potwierdzający)</li></ul>
Wypożyczenie	<ul style="list-style-type: none"><li>• instrukcja obsługi, instrukcja bezpieczeństwa</li><li>• przewód zasilający</li><li>• kabel RS232</li><li>• kabel USB</li><li>• uchwyty kablone</li><li>• podstawki do montażu pionowego (Tower)</li><li>• przewody IEC 10 A – 2 szt.</li><li>• zestaw szyn montażowych do szafy 19"</li></ul>
Karta Web/SNMP	<ul style="list-style-type: none"><li>• Protokoły i certyfikaty cyberbezpieczeństwa: UL 2900-1 / IEC 62443-4-2 / HTTPS / MQTTS / RADIUS / LDAP / SSH/ pakiet szyfrów TLS 1.2 z minimum SHA256</li><li>• certyfikaty CA i PKI</li><li>• prędkość Gigabit Ethernet</li><li>• różne poziomy nadawania dostępu do konta administratora lub użytkownika</li></ul>
Maks. wymiary UPS (szer. x gł. x wys. w mm)	438 x 603 x 86
Maks. wymiary modułu baterijnego 2U (szer. x gł. x wys. w mm)	438 x 603 x 86
Poziom hałasu (przy standardowym obciążeniu)	< 40 dB
Zgodność z normami UE	Deklaracja zgodności CE
Dodatkowe certyfikaty	Raport CB (TUV), ISO 9001 lub równoważna
Gwarancja	Gwarancja producenta min. 24 miesiące

### Oprogramowanie zarządzające do zasilacza awaryjnego typ II

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Oprogramowanie zarządzające	Oprogramowanie producenta oferowanego zasilacza awaryjnego do monitorowania i zarządzania, umożliwiające: <ul style="list-style-type: none"><li>- tworzenie scenariuszy zasilania ukierunkowanych na pojedyncze maszyny wirtualne, grupy maszyn wirtualnych lub automatyczne grupy maszyn wirtualnych</li><li>- tworzenie scenariuszy zasilania ukierunkowanych na klastry, w tym w</li></ul>



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA



## Cyberbezpieczny Samorząd

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	środowiskach hiperkonwergentnych - tworzenie scenariuszy zasilania z sekwencyjnym wyłączaniem poszczególnych maszyn wirtualnych Licencja na oprogramowanie musi być dostosowana do wymaganej w postępowaniu infrastruktury oraz zapewniać wsparcie producenta przez okres do końca czerwca 2026 r.

### XI. Agregat prądotwórczy:

Przedmiotem zamówienia jest agregat prądotwórczy o minimalnym parametrach:

1. Cyfrowa regulacja napięcia  $\pm 0,25\%$
2. Kontrola napięcia na trzech fazach
3. Niski poziom zakłóceń THD  $< 2\%$
4. Prąd startowy prądnicy  $270\% I_n$  (opcjonalnie  $300\%$ )
5. Klasa izolacji H
6. Stopień ochrony prądnicy IP23
7. Klasa wykonania G3 (wg ISO 8528-5)
8. Szybkie przyjęcie obciążenia
9. Gotowość pracy w trybie ręcznym i automatycznym
10. Czas pracy na zbiorniku przy  $75\%$  obciążenia 31,5 h
11. Kompaktowe rozmiary
12. Możliwość podnoszenia wózkiem od przodu i od boku

#### Parametry techniczne – minimalne:

Moc maksymalna ESP 35,0 kVA / 28,0 kW

Moc znamionowa PRP 31,0 kVA / 25,0 kW

Prąd znamionowy PRP 45,0 A

Częstotliwość 50 Hz

Napięcie 400 V

Emisja spalin non-emission

Rodzaj paliwa Diesel (EN 590)

Pojemność zbiornika paliwa 200 l

Zużycie paliwa dla 50% / 75% 100% / 110% PRP - 4 / 5,7 / 7,6 / 8,4 l/h

Autonomia dla 75% / 100% obciążenia - 31,5 / 23,6 h

Waga agregatu bez paliwa – max. 820 kg

Wymiary maksymalne D x S x W 1920 x 1020 x 1600 mm

Moc akustyczna Lwa - maksymalnie 90 dBA

Ciężenie akustyczne z 7m LPa maksymalnie -  $60,5 \pm 1$  dBA



## Cyberbezpieczny Samorząd

### Wyposażenie podstawowe:

#### Silnik:

Moc silnika netto – min. 28,7 kW

Emisja spalin non-emission

Regulacja obrotów – elektroniczna

Klasa wykonania – co najmniej G3 (wg. normy ISO 8528-5 lub równoważnej)

Pojemność silnika – co najmniej 2,3 l

Liczba cylindrów – min. 4

Układ paliwowy – wtrysk bezpośredni

Instalacja – min. 12 V

Pojemność cieczy chłodzącej – min. 9,4 l

Pojemność miski olejowej – min. 9,5 l

Rodzaj paliwa – diesel

#### Prądnica:

Napięcie znamionowe – min. 400V

Współczynnik mocy ( $\cos \varphi$ ) - max. 0,8

Temperatura, wysokość – max. 40 °C, 1000m n.p.m.

Moc znamionowa – max. 32, 0 kVA

Stopień ochrony – min. IP 23

Połączenie z silnikiem - bezpośrednie

Technologia - bezszczotkowa

Podtrzymanie prądu zwarciovego – min. 270% 10s

Sprawność – min. 87%

Klasa izolacji – min. H

Zawartość harmoniczných THD <2 %

Reaktancja  $X_d''$  min. 8 %

Regulacja napięcia AVR, cyfrowy

Pomiar napięcia 3 fazy

Dokładność regulacji +/- 0,25%

#### Sterownik:

- Intuicyjny interfejs graficzny
- Zegar czasu rzeczywistego z akumulatorem
- Kontrola zasilania sieciowego, automatyczny start generatora
- Dziennik zdarzeń: do 350 pozycji



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA



## Cyberbezpieczny Samorząd

- Pomiar wartości prądu w 3 fazach
- Pomiar wartości napięcia sieci i generatora
- Pomiar mocy czynnej, biernej i pozornej
- Licznik energii czynnej i biernej generatora
- Licznik czasu pracy, liczniki przeglądów
- Liczniki wielofunkcyjne, do konfiguracji wg potrzeb
- Pomiar napięcia akumulatora
- Pełne zabezpieczenie silnika i prądnicy
- Magistrala CAN i port USB
- Możliwość doposażenia o dwa dodatkowe moduły komunikacyjne lub wejść/wyjść
- Podłączenie do internetu poprzez moduł Ethernet, GPRS lub 4G (opcja)
- Wsparcie protokołu ModBus oraz SNMP
- Darmowa aplikacja WebSupervisor dla Android lub iOS do podglądu floty agregatów
- Wysyłanie powiadomień o błędach poprzez SMS lub e-mail (wymagany moduł CM-GPRS lub CM-4G-GPS)
- Lokalizacja, funkcja „Geo-fencing”: (wymagany moduł CM-4G-GPS)
- 3 poziomy dostęp, zabezpieczone hasłem
- Moduł PLC umożliwiający rozszerzenie funkcjonalności sterownika wg specyficznego zapotrzebowania
- Dostępne dodatkowe sygnały binarne: wejścia – 2, wyjścia – 1, pomiarowe – 3

Wyłącznik główny agregatu

Cewka wybijakowa wyłącznika

Transformatorowa ładowarka akumulatora

Grzałka bloku silnika

Elektroniczny regulator obrotów

System paliwowy wtrysk bezpośredni

Ramozbiornik 200 l z wanną retencyjną i izolacją dźwiękochłonną

Dwa wlewy paliwa

4 punkty podnoszenia z zawieszami

Wysunięte płozy ułatwiające mocowanie do podłoża

Presostat niskiego ciśnienia oleju

Pomiar ciśnienia oleju

Termostat wysokiej temperatury silnika

Pomiar temperatury silnika

Filtr paliwa z separatorem wod





## Cyberbezpieczny Samorząd

Grzałka silnika z termostatem

Wlew płynu chłodzącego na dachu obudowy

Sygnalizator dźwiękowy awarii

Przycisk awaryjnego zatrzymania

Obudowa wyciszona

Ramozbiornik z przestrzenią retencyjną

Wibroizolatory drgań silnika i prądnicy

Tłumik spalin z kompensatorem drgań

Uchwyty załadunkowe



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA