

---

Zamawiający:

**Gmina Słubice,**

09-533 Słubice, ul. Płocka 32

NIP: 7743210626 REGON: 611015968

[www.slubice.org.pl](http://www.slubice.org.pl)

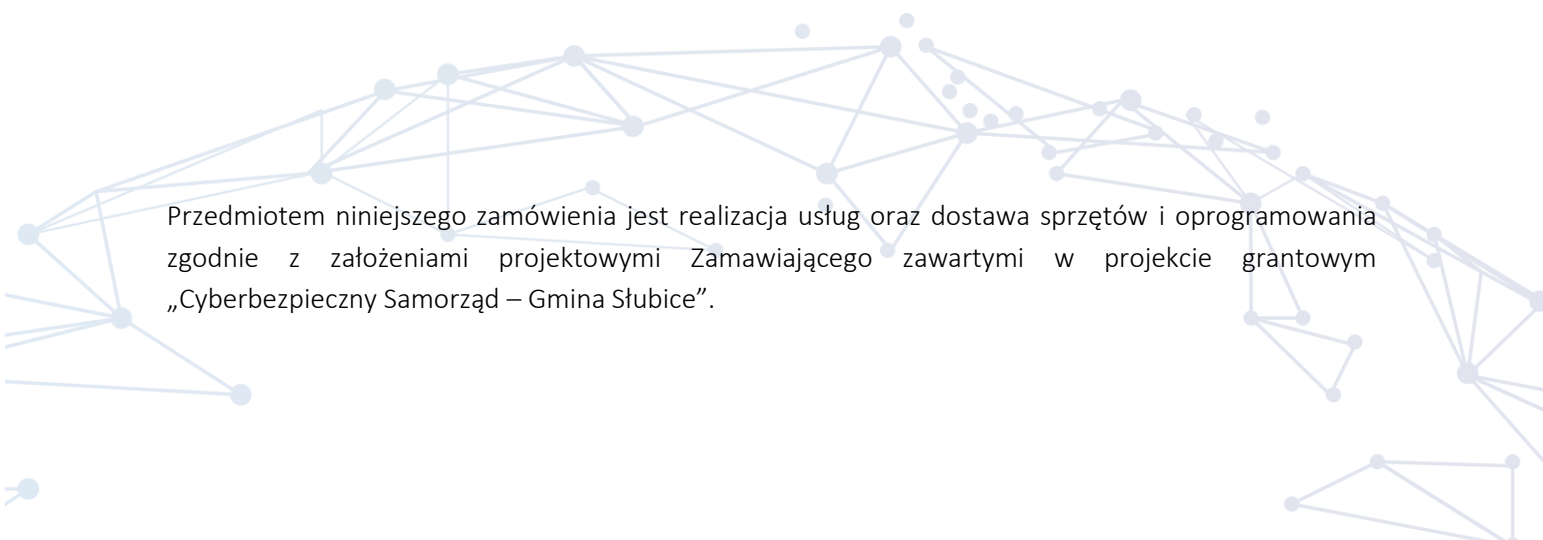
[gmina@slubice.org.pl](mailto:gmina@slubice.org.pl)

(+48) 24 277 89 30

---

## ZAŁĄCZNIK NR 6 DO (SWZ)

# OPIS PRZEDMIOTU ZAMÓWIENIA



Przedmiotem niniejszego zamówienia jest realizacja usług oraz dostawa sprzętów i oprogramowania zgodnie z założeniami projektowymi Zamawiającego zawartymi w projekcie grantowym „Cyberbezpieczny Samorząd – Gmina Słubice”.

## Rozdział I – usługa przeprowadzenia audytów Systemu Zarządzania Bezpieczeństwem Informacji w zgodności z KRI oraz UoKSC dla Urzędu Gminy Słubice (2 szt.)

Zamawiający wymaga przeprowadzenie dwóch audytów Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Gminy Słubice w celu oceny zgodności z wymogami Krajowych Ram Interoperacyjności (KRI) oraz Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UoKSC). Audyty mają na celu zidentyfikowanie potencjalnych luk i ryzyk w zakresie bezpieczeństwa informacji oraz przygotowanie rekomendacji w celu zapewnienia zgodności z wymogami prawnymi i standardami.

Zamawiający wymaga, aby na zespole audytorskim spoczywał obowiązek weryfikacji zgodności z innymi przepisami, w tym:

- zgodność z przepisami dotyczącymi ochrony danych osobowych (np. RODO), w kontekście zarządzania danymi, bezpieczeństwa informacji oraz cyberbezpieczeństwa;
- sprawdzenie zgodności z krajowymi i międzynarodowymi normami oraz standardami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem.

Audyt początkowy SZBI stanowi kluczowy element w ramach projektu Cyberbezpieczny Samorząd, a jego celem jest dokonanie wstępnej oceny obecnego stanu bezpieczeństwa informacji u Zamawiającego, w tym identyfikacja wszelkich zagrożeń, słabości, luk w zabezpieczeniach itd. Na podstawie wyników audytu należy zweryfikować braki i obszary wymagające poprawy, co kluczowe jest dla skutecznego wdrożenia działań w ramach projektu. Audyt początkowy niezbędny jest dla Zamawiającego do oceny zgodności z normami i standardami dotyczącymi zarządzania bezpieczeństwem informacji, a jego wyniki stanowią fundament do opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Audyt końcowy ma za zadanie dla Zamawiającego, aby wykazać efektywność wdrożonych działań i weryfikację czy zidentyfikowane w audycie początkowym słabości i luki zostały skutecznie zlikwidowane, a także czy nowo wdrożone procedury i mechanizmy działają zgodnie z ich założeniami. Zamawiający wymaga, aby audyt końcowy stanowił formalną ocenę funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji i weryfikację jego poprawności, funkcjonowania zgodnie z wymaganiami norm, przepisów prawnych oraz wewnętrznych polityk. Audyt końcowy jest także dla Zamawiającego niezbędny do zapewnienia, że Jednostka jest przygotowana do dalszego funkcjonowania zgodnie z wymogami cyberbezpieczeństwa, a ponadto jego uzasadnienie znajduje się w konieczności formalnego zamknięcia Projektu i jego ocenę.

Zamawiający wymaga przeprowadzenia audytów w formie stacjonarnej

Zamawiający określa szczegółowy zakres audytów:

A. Analiza Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji i zgodności z wymogami KRI oraz UoKSC:

1. Weryfikacja polityk bezpieczeństwa informacji:
  - analiza zgodności polityk bezpieczeństwa informacji z wymaganiami KRI i UoKSC.

- sprawdzenie procedur i instrukcji związanych z zarządzaniem bezpieczeństwem informacji, w tym zarządzania ryzykiem, dostępem, kopiami zapasowymi oraz incydentami bezpieczeństwa.
  - 2. Ocena zgodności z przepisami i wymaganiami prawnymi:
    - sprawdzenie wdrożenia przepisów wynikających z KRI i UoKSC.
    - analiza zgodności z wytycznymi Ministerstwa Cyfryzacji, a także innych standardów i dobrych praktyk w zakresie cyberbezpieczeństwa.
- B. Zarządzanie Dostępem i Bezpieczeństwo Informacji
1. Weryfikacja zarządzania dostępem do systemów i danych:
    - ocena procedur nadawania, modyfikowania oraz odwoływania uprawnień dostępu do systemów informatycznych.
    - weryfikacja autoryzacji użytkowników i zarządzania tożsamością.
  2. Ocena ochrony danych wrażliwych i krytycznych:
    - sprawdzenie mechanizmów kontroli dostępu oraz zabezpieczeń w odniesieniu do danych wrażliwych.
    - weryfikacja stosowanych metod szyfrowania oraz ochrony przed nieautoryzowanym dostępem.
- C. Ocena Świadomości i Przeszkolenia Pracowników
1. Analiza przeprowadzonych szkoleń z zakresu bezpieczeństwa informacji:
    - weryfikacja zgodności programów szkoleniowych z wymaganiami KRI i UoKSC.
    - sprawdzenie świadomości pracowników w zakresie polityk bezpieczeństwa oraz ich wiedzy na temat postępowania w przypadku incydentów.
- D. Zarządzanie Incydentami Bezpieczeństwa i Ryzykiem Cyberbezpieczeństwa
1. Weryfikacja procesów identyfikacji, raportowania i zarządzania incydentami:
    - sprawdzenie zgodności procedur zarządzania incydentami z wymogami KRI i UoKSC.
    - analiza rejestrów incydentów oraz ocena skuteczności działań naprawczych.
  2. Ocena procesów zarządzania ryzykiem:
    - weryfikacja identyfikacji, oceny i dokumentacji ryzyk związanych z bezpieczeństwem informacji.
    - analiza planów zarządzania ryzykiem oraz działań zapobiegawczych i naprawczych.
- E. Weryfikacja Systemów Informatycznych i Technicznych Środków Zabezpieczeń
1. Analiza konfiguracji i zabezpieczeń systemów informatycznych:
    - sprawdzenie aktualizacji, ochrony antywirusowej, firewalli i innych zabezpieczeń technicznych.
    - weryfikacja stosowanych rozwiązań w zakresie szyfrowania i ochrony sieci teleinformatycznej.
  2. Ocena bezpieczeństwa fizycznego i środowiskowego:
    - kontrola zabezpieczeń fizycznych pomieszczeń (serwerowni, biur), w których przetwarzane są dane.
    - weryfikacja zabezpieczeń przeciwpożarowych, systemów monitoringu oraz kontroli dostępu.
- F. Analiza Zarządzania Kopiami Zapasowymi i Odtwarzaniem Danych
1. Ocena procedur tworzenia, przechowywania i odtwarzania kopii zapasowych:
    - weryfikacja zgodności procedur tworzenia kopii zapasowych z wymaganiami KRI i UoKSC.
    - analiza procesów testowania odtwarzania danych i skuteczności tych procesów.

## G. Weryfikacja Procesów Współpracy z Podmiotami Zewnętrznymi i Dostawcami

1. Analiza umów i procedur współpracy z podmiotami trzecimi:
  - sprawdzenie zgodności umów z dostawcami usług IT z wymogami KRI i UoKSC.
  - weryfikacja zapisów dotyczących bezpieczeństwa informacji w relacjach z podmiotami zewnętrznymi.

## 3. Metodyka Przeprowadzenia Audytu:

1. Analiza dokumentacji oraz wewnętrznych polityk i procedur.
2. Wywiady z pracownikami oraz kluczowymi osobami odpowiedzialnymi za bezpieczeństwo informacji.
3. Kontrole na miejscu obejmujące sprawdzenie procesów, systemów i środków technicznych.
4. Testy sprawdzające zgodność z KRI i UoKSC.
5. Przygotowanie raportu z wynikami, analizą ryzyk i rekomendacjami.
3. Oczekiwane Rezultaty:  
Szczegółowe raporty audytowe zawierające:
  - ocenę stanu obecnego.
  - identyfikację niezgodności i obszarów do poprawy.
  - rekomendacje działań naprawczych.

---

## Rozdział II – usługa opracowania pełnej dokumentacji z zakresu Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Gminy Słubice (1 szt.)

Przedmiotem zamówienia jest kompleksowe opracowanie zintegrowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Urzędu Gminy Słubice wraz z wdrożeniem.

Zamawiający wymaga, aby dokumentacja została przygotowana zgodnie z wymaganiami dotyczącymi bezpieczeństwa informacji i systemów informacyjnych dla podmiotów publicznych, określonymi w standardzie NSC 200, a także z uwzględnieniem aktualnie obowiązujących norm międzynarodowych, tj. PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301.

Zamawiający wymaga, aby opracowanie dokumentacji obejmowało m.in.:

1. **Polityki i Procedury dla Systemu Zarządzania Bezpieczeństwem Informacji** - przygotowanie kompleksowych polityk i procedur, które obejmą wszystkie aspekty zarządzania bezpieczeństwem informacji w Urzędzie Gminy w Słubicach. Dokumenty te muszą być opracowane w oparciu o normę PN-EN ISO/IEC 27001 i zawierać m.in.:
  - 1) **Polityka Bezpieczeństwa Informacji** - dokument definiujący cele oraz zasady ochrony informacji, zasady zarządzania bezpieczeństwem oraz zobowiązania organizacji w zakresie ochrony danych.
  - 2) **Polityka Bezpieczeństwa Fizycznego** - opracowanie zasad ochrony dostępu do budynków i pomieszczeń, monitorowanie, zabezpieczanie sprzętu, zarządzanie sytuacjami kryzysowymi oraz regularne szkolenia dla personelu.

- 3) **Polityka Zarządzania Ciągłością Działania** - dokumentacja musi zawierać strategię i plany działania w przypadku zakłóceń w funkcjonowaniu urzędu, gwarantując tym samym ciągłość operacyjną Urzędu Gminy w Słubicach.
2. **Wdrożenie zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji** - realizacja wdrożenia systemu, który obejmie wszystkie istotne elementy bezpieczeństwa, w tym identyfikację i zarządzanie ryzykiem, ochronę danych, monitorowanie incydentów oraz zapewnienie ciągłości działania. Wdrożenie tego systemu jest kluczowe dla Zamawiającego, aby skutecznie chronić dane oraz systemy informatyczne Urzędu Gminy w Słubicach, a także spełnić wymagania prawne i normatywne.
3. **Przegląd i aktualizacja dokumentacji** - wdrożenie mechanizmów regularnego przeglądu i aktualizacji dokumentacji, aby zapewnić jej zgodność z obowiązującymi przepisami prawa oraz standardami międzynarodowymi

Celem opracowania dokumentacji i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji jest stworzenie spójnego, zintegrowanego systemu, który skutecznie zabezpieczy informacje przetwarzane przez Urząd Gminy Słubice, minimalizując ryzyka związane z cyberzagrożeniami, a także zapewni ciągłość operacyjną i zgodność z wymogami prawnymi oraz normatywnymi. Wdrożenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji jest dla Zamawiającego niezbędne dla zagwarantowania, że Urząd Gminy będzie funkcjonował w sposób bezpieczny, zgodny z przepisami oraz odporny na współczesne wyzwania w zakresie cyberbezpieczeństwa.

### Rozdział III – usługa przeprowadzenia szkolenia pracowników z zakresu cyberbezpieczeństwa dla Urzędu Gminy Słubice (2 szt.)

Zamawiający wymaga, aby podczas szkolenia poruszone zostały min. poniższe aspekty:

1. Wprowadzenie do Cyberbezpieczeństwa:
  - definicja i znaczenie cyberbezpieczeństwa;
  - przykłady zagrożeń cybernetycznych w sektorze publicznym;
  - rola pracowników w zapewnieniu bezpieczeństwa informacji.
2. Bezpieczeństwo haseł i zarządzanie dostępem:
  - tworzenie i przechowywanie silnych haseł;
  - zarządzanie dostępem do systemów informatycznych;
  - praktyczne porady dotyczące ochrony danych uwierzytelniających;
3. Phishing i socjotechnika:
  - rodzaje ataków phishingowych i techniki socjotechniczne;
  - jak rozpoznawać podejrzane e-maile i wiadomości;
  - postępowanie w przypadku podejrzenia ataku phishingowego.

#### 4. Bezpieczeństwo pracy zdalnej i mobilnej:

- najlepsze praktyki podczas pracy poza biurem;
- bezpieczne korzystanie z sieci Wi-Fi i urządzeń mobilnych;
- zasady korzystania z urządzeń prywatnych w pracy.

#### 5. Ochrona Danych Osobowych i poufnych informacji:

- podstawowe zasady ochrony danych osobowych (RODO);
- jak bezpiecznie przetwarzać i przechowywać dane wrażliwe;
- przykłady naruszeń danych i konsekwencje prawne.

#### 6. Zabezpieczanie urządzeń i sieci:

- wprowadzenie do podstawowych narzędzi zabezpieczających (antywirus, firewall);
- aktualizacje oprogramowania i dlaczego są ważne;
- zabezpieczanie urządzeń przenośnych i stacji roboczych.

#### 7. Zarządzanie incydentami bezpieczeństwa:

- co to jest incydent bezpieczeństwa i jak go rozpoznać;
- procedura zgłaszania incydentów w Urzędzie Gminy;
- przykłady incydentów i jak można im zapobiegać.

#### 8. Dobre praktyki w codziennej pracy:

- bezpieczne korzystanie z poczty elektronicznej;
- unikanie zagrożeń podczas korzystania z Internetu;
- przechowywanie i niszczenie dokumentów zawierających poufne informacje.

#### 9. Podsumowanie szkolenia:

- przegląd kluczowych zagadnień omówionych podczas szkolenia;
- dyskusja i pytania uczestników;
- przekazanie dodatkowych materiałów edukacyjnych.

Zamawiający wymaga, aby szkolenie online zostało zaprojektowane w taki sposób, aby nie tylko podnosić świadomość w zakresie cyberbezpieczeństwa, ale także rozwijać praktyczne umiejętności uczestników w rozpoznawaniu i neutralizowaniu zagrożeń. Zakres tematyczny bloku szkoleniowego winien być zgodny z wymogami projektu i stanowić integralną część strategii podnoszenia poziomu ochrony informacji w administracji publicznej Urzędu Gminy Słubice.

Zamawiający wymaga także, aby drugie szkolenie obejmowało w swojej tematyce, choć w minimalnym zakresie, kwestie wprowadzanych i wdrażanych rozwiązań oraz urządzeń.



## Rozdział IV – usługa przeprowadzenia szkolenia kadry kierowniczej Urzędu Gminy Słubice z zakresu Systemu Zarządzania Bezpieczeństwem Informacji (1 szt.)

Zamawiający wymaga, aby szkolenie przeprowadzone zostało przez Wykonawcę w minimum dwugodzinnym wymiarze czasowym w formie stacjonarnej w siedzibie Zamawiającego. Zakres szkolenia obejmuje aspekty teoretyczne i praktyczne, zgodne z treścią i zawartością wdrożonej dokumentacji SZBI w Urzędzie Gminy Słubice z uwzględnieniem elementów zabezpieczeń infrastruktury IT.

Zamawiający wymaga, aby podczas szkolenia poruszone zostały kluczowe aspekty systemu, w tym m.in.:

1. Wprowadzenie do Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):

- definicja i znaczenie SZBI;
- podstawowe pojęcia związane z bezpieczeństwem informacji;
- przegląd normy ISO/IEC 27001:2023;
- kluczowe elementy SZBI i ich rola w organizacji;

2. Polityka Bezpieczeństwa Informacji:

- definicja i cel Polityki Bezpieczeństwa Informacji;
- tworzenie, wdrażanie i utrzymanie polityki bezpieczeństwa;
- rola kadry kierowniczej w zarządzaniu polityką bezpieczeństwa;

3. Zarządzanie Ryzykiem:

- proces identyfikacji, analizy i oceny ryzyka;
- metodyka oceny ryzyka zgodnie z ISO/IEC 27005;
- implementacja i monitorowanie środków kontrolnych;

4. Zarządzanie Incydentami Bezpieczeństwa:

- definicja incydentu bezpieczeństwa i jego rodzaje;
- procedury raportowania i reagowania na incydenty;
- role i odpowiedzialności w zarządzaniu incydentami;
- przykłady praktycznych scenariuszy incydentów;

5. Kontrola Dostępu i Zarządzanie Tożsamością:

- zasady kontroli dostępu w organizacji;
- bezpieczne zarządzanie tożsamością użytkowników;
- autoryzacja, autentykacja i monitorowanie aktywności;

6. Świadomość i Szkolenia Pracowników:

- rola edukacji i szkoleń w zapewnieniu bezpieczeństwa informacji;
- tworzenie programu szkoleń z zakresu bezpieczeństwa informacji;
- praktyczne wskazówki dotyczące podnoszenia świadomości pracowników;

7. Audyt i monitorowanie systemu:
  - procedury audytu wewnętrznego SZBI;
  - monitorowanie i przegląd efektywności systemu;
  - rola kadry kierowniczej w zapewnieniu zgodności z wymaganiami;
8. Zarządzanie ciągłością działania:
  - planowanie i wdrażanie strategii ciągłości działania;
  - testowanie i aktualizacja planów ciągłości;
  - integracja zarządzania ciągłością działania z SZBI;
9. Przepisy prawne i regulacyjne:
  - przegląd kluczowych przepisów prawa dotyczących ochrony danych i bezpieczeństwa informacji;
  - obowiązki urzędów gminnych w zakresie zgodności z przepisami;
  - zarządzanie zgodnością z RODO i innymi regulacjami;
10. Rola i odpowiedzialność kadry kierowniczej
  - kluczowe zadania kadry kierowniczej w zakresie zarządzania bezpieczeństwem informacji;
  - budowanie kultury bezpieczeństwa w organizacji;
  - motywowanie i nadzorowanie zespołów odpowiedzialnych za SZBI.

## Rozdział V – dostawa serwera backup wraz z dyskami i oprogramowaniem oraz zasilaniem UPS, a także dostawa biblioteki taśmowej dla Urzędu Gminy Słubice (1 szt.)

Zamawiający wymaga, aby dostarczone urządzenie realizowało wszystkie wymienione poniżej funkcje i wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> <li>Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5"</li> <li>Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.</li> </ul>
Płyta główna	<ul style="list-style-type: none"> <li>Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li> <li>Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci</li> </ul>
Chipset	<ul style="list-style-type: none"> <li>Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych</li> </ul>



Procesor	<ul style="list-style-type: none"> <li>Jeden procesor 8-rdzeniowy, min. 3.2GHz, umożliwiający osiągnięcie wyniku min. 95.1 w teście SPECrate2017_int_base dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> w konfiguracji jednoprosesorowej.</li> </ul>
Pamięć RAM	<ul style="list-style-type: none"> <li>2x16GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 4800MT/s.</li> </ul>
Karta graficzna	<ul style="list-style-type: none"> <li>Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200</li> </ul>
Sloty PCIe	<ul style="list-style-type: none"> <li>Min. 2 sloty PCIe Gen4</li> </ul>
Wbudowane porty/napędy	<ul style="list-style-type: none"> <li>min. 4 porty USB w tym min: <ul style="list-style-type: none"> <li>1 port USB 3.0 z tyłu obudowy,</li> <li>1 port micro USB z przodu obudowy</li> </ul> </li> <li>1 port VGA na tylnym panelu,</li> <li>1 port RS232</li> <li>Napęd LTO7 SAS (zewnętrzny) wraz z: <ul style="list-style-type: none"> <li>5x taśma LTO7</li> <li>1x taśma czyszcząca</li> <li>Kabel połączeniowy SAS do serwera min. 2m</li> </ul> </li> </ul>
Kontroler RAID	<ul style="list-style-type: none"> <li>Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10</li> </ul>
Dyski twarde	<ul style="list-style-type: none"> <li>Zainstalowane <ul style="list-style-type: none"> <li>4x dysk SATA o pojemności min. 4TB, Hot-Plug.</li> </ul> </li> <li>Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.</li> </ul>
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> <li>Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT</li> <li>Czteroportowa karta 12Gb SAS HBA</li> </ul>
Zasilacze	<ul style="list-style-type: none"> <li>Redundantne, o mocy maks. 700W klasy Titanium</li> <li>UPS 1500VA 230V z wyświetlaczem LCD</li> </ul>
Elementy montażowe	<ul style="list-style-type: none"> <li>Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych</li> </ul>
System operacyjny/dodatkové oprogramowanie	<ul style="list-style-type: none"> <li>Windows Server 2022 Standard</li> <li>40x Windows Server 2022/2019 User CALs</li> </ul>
Bezpieczeństwo	<ul style="list-style-type: none"> <li>Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardek.</li> <li>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>Moduł TPM 2.0</li> <li>Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).</li> </ul>
Karta Zarządzania	<ul style="list-style-type: none"> <li>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: <ul style="list-style-type: none"> <li>zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> </ul> </li> </ul>

- o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
  - o szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;
  - o możliwość podmontowania zdalnych wirtualnych napędów;
  - o wirtualną konsolę z dostępem do myszy, klawiatury;
  - o wsparcie dla IPv6;
  - o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
  - o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
  - o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
  - o integracja z Active Directory;
  - o możliwość obsługi przez dwóch administratorów jednocześnie;
  - o wsparcie dla dynamic DNS;
  - o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
  - o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
  - o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
- oraz z możliwością rozszerzenia funkcjonalności o:
- o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
  - o Przesyłanie danych telemetrycznych w czasie rzeczywistym
  - o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze
  - o Automatyczna rejestracja certyfikatów (ACE)

#### Oprogramowanie do zarządzania

- Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:
  - o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
  - o integracja z Active Directory
  - o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
  - o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
  - o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
  - o Szczegółowy opis wykrytych systemów oraz ich komponentów
  - o Możliwość eksportu raportu do CSV, HTML, XLS, PDF
  - o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
  - o Grupowanie urządzeń w oparciu o kryteria użytkownika
  - o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
  - o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
  - o Szybki podgląd stanu środowiska
  - o Podsumowanie stanu dla każdego urządzenia

- Szczegółowy status urządzenia/elementu/komponentu
- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej
- Możliwość przejęcia zdalnego pulpitu
- Możliwość podmontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

#### Oprogramowanie do monitorowania

Opiera na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:

- Monitoring:
  - ilość podłączonych oraz rozłączonych systemów
  - stan podłączonych urządzeń
  - informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów

- Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
- informacje o statusie gwarancji dla poszczególnych urządzeń
- informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
- informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
- Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych
- Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
- Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
- Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
- Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
- Monitoring parametrów serwerów z informacją o minimum:
  - Obciążeniu procesora
  - Zużyciu pamięci RAM
  - Temperaturze procesorów
  - Temperaturze powietrza wlotowego
  - Zużyciu prądu
  - Zmianach w fizycznej konfiguracji serwera
  - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Monitoring parametrów pamięci masowych z informacją o minimum:
  - Opóźnieniach
  - IOPS
  - Przepustowości
  - Utylizacji kontrolerów
  - Pojemności całkowita i dostępna
  - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
  - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
  - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
  - Informacje o poziomie redukcji danych
  - Informacje o statusie replikacji oraz snapshotów

- Monitoring parametrów przełączników sieciowych z informacją o minimum:
  - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
  - Stanie komponentów: zasilacze, wentylatory
  - Podłączonych hostach
  - Ilości i statusu portów
  - Utylizacji procesora
  - Utylizacji poszczególnych portów
  - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Aktualizacja firmware
  - możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
  - Możliwość generowania raportów dla serwerów zawierających informację o:
    - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
    - Średnim obciążeniu: procesorów, pamięci RAM, IO,
  - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
    - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
  - Generowanie raportów do plików CSV i PDF
- Cyberbezpieczeństwo
  - Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
  - Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.

- Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
  - Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.
- Wspierane urządzenia
  - Urządzenie Producenta dostarczane w ramach postępowania
  - Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)
- Wirtualny asystent
  - Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;
- Możliwość rozszerzenia funkcjonalności
  - Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
- Inne
  - Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
- Certyfikaty
  - Oferowana platforma musi być zaprojektowana zgodnie ze standardami:
    - ISO 27001
    - NIST Security and Privacy Controls for Federal Information Systems and Organization
    - CSA Cloud Control Matrix

## Certyfikaty

- Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001
- Serwer musi posiadać deklaracja CE.
- Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.



	<ul style="list-style-type: none"> <li>– Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.</li> </ul>
Dokumentacja użytkownika	<ul style="list-style-type: none"> <li>– Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</li> <li>– Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li> </ul>
Warunki gwarancji	<ul style="list-style-type: none"> <li>– Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 2 lat.</li> <li>– Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</li> <li>– Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)</li> <li>– Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</li> <li>– Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</li> <li>– Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li> <li>– Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>– Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.</li> <li>– Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</li> <li>– Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: <ul style="list-style-type: none"> <li>o Możliwości utworzenia zgłoszenia serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.</li> <li>o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub</li> </ul> </li> </ul>

części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.

- Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
- Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
- Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaze dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

## Rozdział VI – dostawa agregatu prądotwórczego dla Urzędu Gminy Słubice (1 szt.)

Zamawiający wymaga, aby generator prądotwórczy (agregat) pochodził z seryjnej, bieżącej produkcji (klas wykonania min. G2) i był wykonany zgodnie z obowiązującymi normami i standardami, w szczególności w zgodności z normą PN/EN ISO 8528-13:2016-07, PN-EN ISO 3744:2011, ISO 8528-1:2005, Dyrektywą 2006/42/WE Parlamentu Europejskiego i Rady (Dyrektywa Maszynowa), Dyrektywą 2000/14/WE Parlamentu Europejskiego i Rady oraz Dyrektywą 2005/88/WE (Dyrektywa Hałasowa), a także 2014/30/UE oraz 2014/35/UE sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia.

Zamawiający wymaga, aby generator prądotwórczy (agregat) spełniał wszystkie wymienione powyżej wymagania:

- moc znamionowa agregatu – 100kVA (80 kW);
- moc awaryjna agregatu nie mniej niż – 110 kVA (88 kW).
- napięcie – 400/230 V.
- częstotliwość – 50Hz.
- agregat w wersji obudowanej.

Zamawiający wymaga, aby generator prądotwórczy (agregat) wyprodukowany był w Polsce i posiadał oznaczenie CE. Ponadto urządzenie musi być w całości spreparowane przez jednego producenta, który powinien posiadać wdrożony system ISO 9001:2015, system AQAP 2110:2016. Zamawiający nie dopuszcza jakichkolwiek modyfikacji urządzenia ingerujących w jego konstrukcję.

Zamawiający określa szczegółowe parametry generatora prądotwórczego (agregatu):

- obudowa agregatu i jego konstrukcja:
  - wymagana obudowa dźwiękochłonna, wyciszona specjalną, niepalną pianką wygłuszającą;
  - wymagana obudowa wyposażona w niezbędne cztery drzwi dostępne na dłuższych bokach;
  - wymagany wylot spalin i gorącego powietrza poprzez górną połą obudowy;
  - wymagane podejście kablowe umiejscowione na dłuższym boku po lewej stronie, bezpośrednio pod wyłącznikiem głównym agregatu (dla umożliwienia wprowadzenia okablowania bez konieczności wychodzenia kablami poza obrys agregatu);
  - wymagana bardzo mocna konstrukcja z możliwością transportu wózkiem widłowym, dźwigiem, HDS – na pasach, widłach lub łańcuchach;
  - wymagana rama izolowana od podłoża za pomocą gumowych stóp (stożków) przykręconych do ramy, służących także regulacji wysokości (poziomowania);
  - wymagana obudowa z awaryjnym, zewnętrznym przyciskiem zatrzymania;
  - wymagane wysokowydajne amortyzatory drgań silnika i prądnicy;
  - wymagane wymiary nieprzekraczające 3200 mm długości, 1100 mm szerokości, 1845 mm wysokości;
  - wymagany stalowy tłumik dźwięków -35db(A) – zabudowany wewnątrz agregatu.
- zaciski na listwie sterowniczej:
  - wymagany styk NC do podłączenia okablowania zewnętrznego stopu pożarowego;
  - wymagany dla podłączenia okablowania potrzeb własnych agregatu;
  - wymagany dla podłączenia okablowania sterowania układem SZR.
- zbiornik paliwa, czujnik poziomu paliwa, alarmy itd:
  - wymagana pojemność zbiornika paliwa wynosząca co najmniej 260 L;
  - wymagany zbiornik umiejscowiony w ramie agregatu;
  - wymagany zbiornik pozwalający na ciągłą pracę agregatu przez co najmniej 16,7 h przy obciążeniu 75%;
  - wymagany zbiornik pozwalający na ciągłą pracę agregatu przez co najmniej 12,3 h przy obciążeniu 100%;
  - wymagany pojemnościowy czujnik poziomu paliwa z procentowym wskazaniem na sterowniku;
  - wymagana sygnalizacja alarmowa przy poziomie rezerwy (15% poziomu paliwa);
  - wymagane zabezpieczenie przed zapowietrzeniem – wyłączenie agregatu przy osiągnięciu 5% paliwa;
  - wymagany korek spustowy zbiornika oraz co najmniej jeden niezależny otwór w zbiorniku zaślepiony deklek na śrubach, umożliwiający montaż i podłączenie dodatkowej instalacji paliwowej, bądź przeniesienie wlewu paliwa na drugą stronę zbiornika.
- jednostka napędowa:
  - wymagany silnik diesla;
  - wymagana moc znamionowa PRP nie mniejsza niż 90 kW;
  - wymagana liczba i układ cylindrów – 4 L;
  - wymagany bezpośredni typ wtrysku paliwa;
  - wymagana elektroniczna regulacja obrotów;
  - wymagana misja spalin – min. Stage II;
  - wymagane podgrzewanie bloku – grzałka silnika kontrolowana przez sterownik agregatu;
  - wymagany korek wlewu paliwa zamykany kluczykiem, wewnątrz obudowy;
  - wymagany suchy filtr powietrza;
  - wymagany silnik chłodzony glikolem;
  - prędkość obrotowa – 1500 r.p.m.;
  - układ elektryczny 12 V;

- akumulator 12 V;
  - automatyczna ładowarka buforowa akumulatora/ów 12V/5A w czasie czuwania;
  - osłona elementów gorących oraz ruchomych;
  - spalanie przy 75% obciążenia nie więcej niż – 16,2 l/h;
  - spalanie przy 100% obciążenia nie więcej niż – 22,0 l/h.
- prądnica:
    - wymagana automatyczna regulacja napięcia;
    - obudowa IP23 (zgodnie z IEC-34-5);
    - złącze – elastyczny dysk;
    - klasa izolacji H;
    - wytrzymałość zwarcia prądnicy >300% obciążenia znamionowego;
    - wymagane wykonanie, gdzie stojan prądnicy jest nawinięty z poskokiem 2/3, dla zapewnienia eliminacji krotności trzeciej harmonicznej (3, 9, 15, itd.) napięcia wyjściowego. Poskok 2/3 minimalizuje indukowanie się nadmiernych prądów w obwodzie neutralnym.
  - sterownik z pełną obsługą rozwiązań producenta, z komunikatami w języku polskim:
    - wymaga się, aby sterownik pozwalał na kontrolę parametrów sieci i agregatu (napięcie, prądów, mocy, częstotliwości,  $\cos \phi$ , napięcia ładowania akumulatora, ilość paliwa w zbiorniku, czasu pracy agregatu, parametrów silnika);
    - wymaga się, aby panel sterownika wyposażony był w tabliczkę z diodami sygnalizacyjnymi dla łatwej obsługi i szybkiej identyfikacji stanów pracy urządzenia;
    - wymagana jest identyfikacja alarmów dotyczących działania baterii, pracy alternatora, poziomu paliwa, ciśnienia oleju oraz dwa dodatkowe do zdefiniowania;
    - wymaga się, aby sterownik posiadał w tylnej ścianie wolne sloty do podłączenia dodatkowych modułów sygnalizacyjnych np. GSM, ETHERNET, styków/wyjść przekaźnikowych dla sygnałów bezpotencjałowych (do zdefiniowania przez użytkownika);
    - wymaga się, aby szafa elektryczna/automatyki agregatu była zbudowana na podzespołach renomowanych producentów elektryki i elektroniki, według norm i standardów.

Zamawiający wymaga, aby sterownik – ekonomiczny kontroler agregatu gotowy do integracji BMS i monitorowania przez Internet, posiadał cechy:

- obsługa agregatów na olej napędowy i gaz;
- obsługa 400 Hz;
- dziennik - 400 zdarzeń;
- możliwość edycji wszystkich parametrów na panelu przednim;
- 3-poziomowe hasło konfiguracyjne;
- graficzny wyświetlacz LCD, min. 128x64;
- języki do pobrania (domyślnie – polski);
- wyświetlanie przebiegów napięcia i prądów;
- analiza harmonicznych;
- wyjścia 16 A MCB i GCB;
- 8 konfigurowalnych wejść cyfrowych;
- wejścia rozszerzalne do 40;
- 6 konfigurowalnych wyjść cyfrowych;
- wyjścia z możliwością rozszerzenia do 38;
- 3 konfigurowalne wejścia analogowe;
- zarówno CANBUS-J1939, jak i MPU;
- 3 konfigurowalne alarmy serwisowe;
- tygodniowy harmonogram pracy;

- ręczna „precyzyjna regulacja prędkości” w wybranych ECU;
- automatyczne sterowanie pompą paliwa;
- ochrona przed nadmierną mocą;
- odwrotna ochrona zasilania;
- zabezpieczenie przed przeciążeniem IDMT;
- zrzut obciążenia, obciążenie zastępcze;
- zarządzanie wieloma obciążeniami;
- zabezpieczenie od asymetrii prądu;
- ochrona przed asymetrią napięcia;
- zegar czasu rzeczywistego z podtrzymaniem bateryjnym;
- kontrola prędkości biegu jałowego;
- ładowanie akumulatora włączone;
- wiele parametrów nominalnych;
- napęd Tactor i MCB;
- 4 kwadrantowe liczniki mocy agregatu;
- liczniki zasilania sieciowego;
- wskazania poziomu paliwa;
- wyświetlacz diagnostyczny modemu;
- konfigurowalny przez USB, RS-485 i GPRS;
- darmowy program konfiguracyjny;
- gotowy do centralnego monitorowania;
- obsługa mobilnych agregatów prądotwórczych;
- łatwa aktualizacja oprogramowania sprzętowego USB;
- stopień ochrony IP65 ze standardową uszczelką.

#### Pomiary:

- napięcia sieci i agregatu PN / PP;
- częstotliwość sieci i agregatu;
- prądy fazowe sieci i agregatu;
- prądy neutralne sieci i agregatu;
- sieć i agregat, faza i suma, kW, kVA, kVAR, pf;
- prędkość silnika;
- napięcie baterii;
- temperatura silnika;
- ciśnienie oleju;
- zużycie paliwa (dla silników wyposażonych w ECU).

#### Komunikacja:

- 4-pasmowy modem GPRS;
- port USB;
- RS-485 (2400-115200);
- RS-232 (2400-115200);
- J1939-CANBUS;
- centralny monitoring internetowy;
- wysyłanie wiadomości SMS;
- wysyłanie e-mail;
- darmowe oprogramowanie na PC: Rainbow Plus;
- Modbus RTU.

Zamawiający wymaga, aby agregat zapewniał monitorowanie pracy za pomocą GPS, tj. zapewniał wysyłanie sygnałów alarmowych z wykorzystaniem sieci GSM na trzy podane telefony komórkowe. Wymagane są co

CENTRUM PROJEKTÓW POLSKA CYFROWA  
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cpcp@cpcp.gov.pl

najmniej 4 sygnały alarmowe: start agregatu (po zaniku sieci), niski poziom paliwa (rezerwa), stop agregatu (po powrocie sieci), awaria agregatu (alarm globalny).

Zamawiający wymaga, aby urządzenie posiadało układ SZR (160A) typu RTSE lub równoważny, na przełączniku z napędem silnikowym. Układ automatyczno-elektryczny, do samodzielnego przełączania zasilania do toru rezerwowego – prądotwórczego, gdy na torze podstawowym nastąpi anomalia napięcia lub jego zanik. Po przywróceniu napięcia toru podstawowego układ powinien wykonać automatyczny powrót zasilania do stanu pierwotnego. Układ powinien składać się z dwóch niezależnych rozłączników izolacyjnych ze wspólnym napędem silnikowym, z możliwością przełączania elektrycznego w trybie automatycznym oraz ręcznego przy pomocy dołączonej ręczki. Układ SZR musi posiadać funkcję „zrzut obu zasilan” oraz zaciski na listwie sterowniczej dla podłączenia kabla, sygnału z wyłącznika pożarowego (głównego) obiektu.

Sterownik agregatu powinien zawierać tryby sterowania:

- sterowanie automatyczne;
- powrót napięcia;
- sterowanie ręczne mechaniczne.

Zamawiający wymaga dla pełnego wsparcia, aby:

- dostawca całości urządzeń i usług w ramach zadania Cyberbezpieczny Samorząd posiadał umowę o współpracy z producentem agregatu w zakresie dostawy, uruchomienia i serwisowania dostarczonych maszyn i urządzeń dodatkowych;
- producent agregatu posiadał w Polsce co najmniej 10 lat własny oddział, serwis oraz magazyn części zamiennych i materiałów eksploatacyjnych.

Zamawiający wymaga, aby przed dostarczeniem agregatu istniała możliwość wykonania próby FAT u producenta, w obecności komisji zamawiającego i aby dokumentacja z próby fabrycznej – próby FAT- stanowiła protokół do dokumentacji powykonawczej.

## Rozdział VII – dostawa urządzeń UPS stanowiskowych dla Urzędu Gminy Słubice (12 szt.)

Zamawiający wymaga, aby dostawa obejmowała 12 szt. urządzeń (min. 1200VA/600W każdy) wykonanych w topologii VI (line-interactive) z minimalną baterią (2 szt. 12V 7Ah), które umożliwiają podtrzymanie pracy przy 50% obciążeniu (300W) na czas nie krótszy niż 11 minut.

Parametr	Wymagania minimalne
moc pozorna	min. 1200VA
moc rzeczywista	min. 600W
Technologia	VI (line interactive)
Typ obudowy	wolnostojąca
praca sieciowa	
Napięcie wejściowe	170 ÷ 280 V AC ± 7 %
Częstotliwość napięcia wejściowego	45 ÷ 55 Hz ± 1 Hz
Zakres napięcia wyjściowego	230 V AC ± 10 %
Kształt napięcia wyjściowego	Schodkowa aproksymacja sinusoidy / Tak jak na wejściu
Progi przełączania sieć – UPS	170 ÷ 280 V AC ± 7 %



Czas przełączania sieć – UPS	<6ms
praca bateryjna	
Napięcie wyjściowe	~230V ± 10%
Częstotliwość napięcia wyjściowego	50Hz ± 1Hz
Kształt napięcia wyjściowego na pracy bateryjnej	Schodkowa aproksymacja sinusoidy
Progi przełączania UPS – sieć	176 V ÷ 274 V AC ± 7 %
Zabezpieczenie wyjściowe przeciwzwarcowe	elektroniczne
Zabezpieczenie wyjściowe przeciążeniowe	elektroniczne
Czas podtrzymania (P 0,8max/P 0,5max)	minimum 4,5 / 11 min
akumulatory wewnętrzne	minimum 2szt 12V 7Ah; szczelne, bezobsługowe
pozostałe	
wejscie zasilania	IEC320 C14
Ilość i typ gniazd wyjściowych	minimum 2 x PN-E-93201 oraz 2 x IEC 320 C13 (10 A)
Filtr telekomunikacyjny	minimum filtr RJ45 (LAN 10/100 Base-T)
Sygnalizacja	Akustyczno-optyczna, w tym minimum wyświetlacz LCD sygnalizujący napięcie wejściowe i wyjściowe, poziom obciążenia, stan naładowania baterii
Zimny Start	tak
Interfejs komunikacyjny	USB (kabel w komplecie)
Waga UPS	do 9kg
wymiary	nie większe niż: wysokość 195mm; szerokość 139mm; głębokość 365mm
gwarancja	min 24 miesiące na elektronikę i 12 miesięcy na akumulatory;
serwis	autoryzowany serwis producenta zlokalizowany w Polsce. serwis realizowany w systemie door-to-door
oprogramowanie	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania) wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
certyfikaty producenta (załączyć do oferty)	ISO 9001:2008 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania;
	deklaracja CE producenta sprzętu
oświadczenia / dokumenty	Zamawiający wymaga oświadczenie producenta, że dostarczany sprzęt będzie pochodził z oficjalnego kanału sprzedaży, fabrycznie nowy, wyprodukowany w 2024 roku.

	Zamawiający wymaga oświadczenie producenta o możliwości udostępnienia przed dostawą 1 sztuki wyrobu na testy w ciągu 3 dni roboczych od wezwania przez zamawiającego.
	Zamawiający wymaga oświadczenie producenta o posiadaniu licencji oraz pełnych praw do oprogramowania do monitorowania pracy UPS.
	Zamawiający wymaga dostarczenia karty katalogowa oferowanego sprzętu.

## Rozdział VIII – dostawa oprogramowania antywirusowego dla Urzędu Gminy Słubice (2 lata, 30 licencji)

Zamawiający wymaga, aby dostarczone oprogramowanie obejmowało 30 licencji na stanowiska komputerowe oraz 2 licencje dla serwerów na okres 2 lat i spełniało poniższe wymagania.

Ochrona antywirusowa wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Rozwiązanie dla ochrony antywirusowej stacji roboczych musi wspierać następujące systemy operacyjne:

- ✓ Microsoft Windows 10;
- ✓ Microsoft Windows 11;
- ✓ macOS version 14 "Sonoma";
- ✓ macOS version 13 "Ventura";
- ✓ macOS version 12 "Monterey".

Rozwiązanie dla ochrony antywirusowej systemów serwerowych musi wspierać następujące systemy operacyjne:

- ✓ Microsoft® Windows Server 2016 Standard;
- ✓ Microsoft® Windows Server 2016 Essentials;
- ✓ Microsoft® Windows Server 2016 Datacenter;
- ✓ Microsoft® Windows Server 2016 Core;
- ✓ Microsoft® Windows Server 2019 Standard;
- ✓ Microsoft® Windows Server 2019 Essentials;
- ✓ Microsoft® Windows Server 2019 Datacenter;
- ✓ Microsoft® Windows Server 2019 Core;
- ✓ Microsoft® Windows Server 2022 Standard;

- ✓ Microsoft® Windows Server 2022 Essentials;
- ✓ Microsoft® Windows Server 2022 Datacenter;
- ✓ Microsoft® Windows Server 2022 Core.

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

- ✓ Microsoft Edge;
- ✓ Mozilla Firefox;
- ✓ Google Chrome;
- ✓ Safari.

Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów muszą posiadać Polski interfejs użytkownika.

Ten sam agent zainstalowany na systemach Windows musi umożliwiać rozbudowę funkcjonalności

o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy muszą być zarządzane z tej samej konsoli zarządzającej

#### Opis technologii

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
2. Rozwiązanie musi posiadać wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
3. Rozwiązanie musi wspierać technologię Antimalware Scan Interface (AMSI)
4. Rozwiązanie musi umożliwiać wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
5. W momencie wykrycia infekcji rozwiązanie musi automatycznie starać się wyleczyć plik, a jeśli nie jest to możliwe przenosić go do bezpiecznego folderu kwarantanny.
6. Rozwiązanie musi posiadać możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwalając na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
7. Rozwiązanie musi chronić plik systemowy HOSTS przed nieautoryzowanymi zmianami.
8. Rozwiązanie musi posiadać mechanizmy skanujące dyski sieciowe.
9. Skanowanie dysków sieciowych musi być możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.

10. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
11. Rozwiązanie musi posiadać mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
12. Musi istnieć możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
13. Wymagane aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, umożliwiające zarówno aktualizację automatyczną programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
14. Uaktualnienia definicji wirusów posiadające podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
15. Rozwiązanie posiadające możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
16. Wymagana aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następująca w sposób automatyczny, niewidoczny dla użytkownika końcowego.
17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymagająca dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następująca automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
18. Rozwiązanie posiadające możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
19. Rozwiązanie posiadające możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
20. Rozwiązanie posiadające możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
21. Rozwiązanie posiadające możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
22. Rozwiązanie posiadające możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
23. Rozwiązanie posiadające możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
24. Rozwiązanie posiadające możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
25. Skanowanie dysków przenośnych odbywające się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.
26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymagająca zatrzymania procesu skanowania na jakimkolwiek systemie.
27. Rozwiązanie posiadające funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym

28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
30. Rozwiązanie posiadające heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
31. Umożliwianie wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
32. Rozwiązanie posiadające mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujące na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
33. Rozwiązanie posiadające technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie powinny być wysyłane do analizy w infrastrukturze producenta.
34. Rozwiązanie posiadające technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
35. Rozwiązanie posiadające możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
36. Rozwiązanie posiadające możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
37. Rozwiązanie posiadające możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
38. Rozwiązanie posiadające możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
39. Rozwiązanie automatycznie powiadamiające użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
40. Rozwiązanie posiadające możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
41. Rozwiązanie posiadające możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
42. Rozwiązanie umożliwiające blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
44. Rozwiązanie posiadające możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej

informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.

45. Rozwiązanie wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamianie skrypty ActiveX i pobierane pliki.
46. Rozwiązanie posiadające możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
47. Rozwiązanie umożliwiające blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
48. Oprogramowanie zapewniające co najmniej 30 kategorii klasyfikacji witryn WWW.
49. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, musi być powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
50. Rozwiązanie umożliwiające blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
51. Rozwiązanie posiadające wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokujące możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokujące zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
54. Kontrola połączenia umożliwiająca zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator musi mieć możliwość tworzenia własnej listy takich witryn.
55. Rozwiązanie posiadające wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
56. Rozwiązanie posiadające funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
57. Profile bezpieczeństwa zapory ogniowej zawierające predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
58. Rozwiązanie pozwalające na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
59. Rozwiązanie posiadające możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
60. Rozwiązanie umożliwiające stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.



61. Rozwiązanie musi być wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
63. Moduł aktualizacji aplikacji, okresowo skanujący aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
64. Moduł aktualizacji aplikacji pełniący rolę mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
65. Administrator posiadający możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
66. Administrator posiadający możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
67. Mechanizm aktualizacji aplikacji umożliwiający automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator musi posiadać możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
69. Administrator konsoli zarządzającej musi mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
70. Mechanizm aktualizacji aplikacji (patch management) nie wymagający uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
71. Administrator musi mieć możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
72. Rozwiązanie umożliwiające wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
73. System centralnego zarządzania prezentujący niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
74. Oprogramowanie umożliwiające blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
75. Mechanizm kontroli urządzeń zewnętrznych wspierający m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
76. Oprogramowanie umożliwiające zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.

77. Lista urządzeń zaufanych musi być tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
78. Rozwiązanie posiadające możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
79. Mechanizm kontrolujący urządzenia umożliwiające blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
80. Rozwiązanie posiadające opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
81. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
82. Rozwiązanie posiadające możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
83. Rozwiązanie pozwalające na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
84. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiadające możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
85. Rozwiązanie pozwalające na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
86. Administrator w konsoli zarządzającej posiadający dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
87. Rozwiązanie posiadające wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
88. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
89. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
90. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
91. Administrator musi mieć możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
92. Administrator musi posiadać możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
93. Rozwiązanie musi być wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu musi polegać na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
94. Moduł musi posiadać możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.

95. Administrator musi posiadać możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
96. Musi istnieć możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
97. Rozwiązanie musi potrafić automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
98. Rozwiązanie musi posiadać funkcjonalność kontroli uruchamianych aplikacji.
99. Tryb kontroli aplikacji musi umożliwiać uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji
100. Musi istnieć możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
101. Tworzone reguły dotyczyć mają czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
102. Na wspieranych systemach Windows rozwiązanie musi pozwalać na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.
103. Administrator musi posiadać w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN
104. Rozwiązanie musi pozwalać na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)
105. Administrator musi mieć możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
106. Rozwiązanie musi pozwalać na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne połączenie za pomocą usług Microsoft RDP (Remote Desktop).
107. Wygenerowany plik może być otwarty i wykorzystany do zdalnego połączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.

#### Centralna administracja

1. Portal zarządzający dostępny w języku polskim.
2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywająca się w formie zaszyfrowanej.
3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.

4. Interfejs zarządzania musi posiadać funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamiania o zakończeniu licencji.
5. Interfejs musi być wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
6. Wykresy muszą być interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
7. Rozwiązanie musi posiadać dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
8. Musi istnieć możliwość eksportu listy wszystkich hostów do pliku CSV.
9. Administrator musi mieć możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. Administrator musi mieć możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie musi posiadać dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
13. Musi istnieć możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego muszą zawierać liczbę i typ hostów, na których został wykryty brak danej poprawki.
15. Po wskazaniu danej poprawki administrator musi posiadać możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
16. Administrator musi mieć możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
17. Rozwiązanie musi posiadać moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie musi posiadać wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator musi widzieć w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. Portal zarządzający musi umożliwiać dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.

22. Dodanie klucza licencyjnego musi skutkować aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie musi mieć możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
26. W przypadku automatycznego przypisywania profili, system musi pozwalać na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
27. Musi istnieć możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
28. Rozwiązanie musi pozwalać administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
29. Z poziomu portalu zarządzającego musi istnieć możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
30. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
31. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
32. Administrator musi posiadać możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.
33. Administrator musi posiadać do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.
34. Portal zarządzający musi pozwalać na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
35. Konsola musi posiadać możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
36. W ramach posiadanych licencji musi istnieć możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.

#### Wdrożenie i szkolenie dotyczące ochrony antywirusowej

##### 1. Wdrożenie

1. Przygotowanie do wdrożenia
  - ✓ Analiza istniejącego środowiska IT, obejmująca stacje robocze oraz serwery, aby upewnić się, że spełniają wymagania systemowe.
  - ✓ Opracowanie planu wdrożenia, uwzględniającego zdalną instalację oprogramowania i konfigurację poszczególnych elementów systemu.



- ✓ Przygotowanie niezbędnych zasobów, takich jak konta użytkowników oraz dostęp do urządzeń końcowych.
- 2. Instalacja i konfiguracja oprogramowania
  - ✓ Zdalna instalacja agentów antywirusowych na 30 stacjach roboczych oraz 2 serwerach.
  - ✓ Konfiguracja centralnej konsoli zarządzającej, dostępnej przez przeglądarkę internetową, bez konieczności instalacji dodatkowych komponentów, takich jak baza danych czy serwer HTTP.
  - ✓ Ustawienie podstawowych parametrów ochrony oraz, w razie potrzeby, konfiguracja dodatkowych funkcji, takich jak zarządzanie podatnościami czy funkcje EDR (Endpoint Detection and Response).
- 3. Testy funkcjonalne
  - ✓ Przeprowadzenie zdalnych testów działania ochrony antywirusowej na wybranych urządzeniach, aby zweryfikować skuteczność i poprawność konfiguracji.
  - ✓ Testowanie automatycznych aktualizacji baz wirusów oraz aktualizacji oprogramowania.
  - ✓ Symulowanie scenariuszy zagrożeń (np. ataków typu ransomware) i monitorowanie reakcji systemu.
- 4. Dostosowanie konfiguracji
  - ✓ Personalizacja ustawień ochrony dla różnych grup urządzeń (stacje robocze, serwery, laptopy).
  - ✓ Konfiguracja harmonogramu skanowania oraz wykluczeń dla specyficznych plików i aplikacji.
  - ✓ Ustalenie zasad aktualizacji oraz powiadomień o zagrożeniach.
- 5. Finalizacja wdrożenia
  - ✓ Zdalna weryfikacja wdrożonego rozwiązania i przeprowadzenie testów końcowych.
  - ✓ Dokumentacja konfiguracji systemu oraz przygotowanie środowiska do codziennego użytkowania.
  - ✓ Zapewnienie wsparcia technicznego po wdrożeniu przez pierwsze trzy miesiące.
- 2. Szkolenie
  - 1. Szkolenie dla administratorów systemu
    - o Czas trwania: 1 dzień (ok. 6-8 godzin).
    - o Zakres szkolenia:
      - ✓ Zarządzanie centralną konsolą, monitorowanie stanu bezpieczeństwa oraz administrowanie licencjami.
      - ✓ Tworzenie i zarządzanie politykami bezpieczeństwa oraz konfiguracją modułów ochrony.
      - ✓ Reakcja na zagrożenia oraz rozwiązywanie problemów związanych z incydentami bezpieczeństwa.
    - o Forma szkolenia: Zdalne wykłady teoretyczne z elementami ćwiczeń praktycznych.
- 3. Dokumentacja i wsparcie powdrożeniowe
  - Opracowanie szczegółowej dokumentacji wdrożenia, obejmującej instrukcje obsługi dla administratorów oraz użytkowników końcowych.



- Przygotowanie procedur postępowania w przypadku wykrycia zagrożeń oraz procedur zarządzania aktualizacjami.
- Świadczenie zdalnego wsparcia technicznego przez okres 24 miesięcy po zakończeniu wdrożenia, aby zapewnić płynne działanie systemu oraz reagowanie na ewentualne incydenty.

Zamawiający zezwala, aby wdrożenie i szkolenie zostało zrealizowane całkowicie zdalnie, co umożliwia elastyczne dostosowanie działań do harmonogramu i potrzeb organizacji, jednocześnie minimalizując wpływ na bieżącą działalność.

---

#### PODSUMOWANIE OPISU PRZEDMIOTU ZAMÓWIENIA

---

Zamawiający wymaga, aby wszystkie oferowane przez Wykonawcę urządzenia i sprzęty były nowe, a także aby pochodziły z oficjalnego kanału dystrybucyjnego w Polsce.

Zamawiający wymaga, aby wszystkie oferowane przez Wykonawcę oprogramowania pochodziły z oficjalnych kanałów dystrybucyjnych w Polsce.

---

Zamawiający wymaga, aby Wykonawca zapewnił, w ramach realizacji przedmiotu umowy za wynagrodzeniem ujętym w przedłożonej ofercie w formularzu ofertowym, zarówno transport jak i rozładunek dostarczanego sprzętu. Wykonawca zobowiązany jest ponadto do wniesienia dostarczonego sprzętu do pomieszczenia wskazanego przez Zamawiającego. Zamawiający informuje natomiast, że we własnym zakresie dokona usunięcia elementów opakowania zbiorczego, w szczególności kartonów, papieru i folii.

---

Zamawiający informuje, że dopuszcza rozwiązania równoważne. W przypadku stwierdzenia użycia w postępowaniu nazw własnych, znaków towarowych lub określeń w sposób bezpośredni wskazujących typ, model, pochodzenie bądź konkretnego producenta - Zamawiający informuje, że stanowią one określenia materiałów, sprzętów czy innych powszechnie dostępnych, które stanowią określenie pożądanej jakości oraz efektu docelowego. Należy przyjąć charakterystyczne dla danego materiału parametry jako odniesienie do standardu określonego przez Zamawiającego.

---

Zamawiający informuje, że Wykonawcy przysługuje prawo do użycia materiału, urządzenia czy wyrobu równoważnego, spełniającego wymagania jakościowe i funkcjonalne opisane w postępowaniu.

W związku z powyższym Zamawiający nie narzuca użycia materiałów, wyrobów czy urządzeń żadnego konkretnego producenta czy dostawcy. Zaproponowane rozwiązania równoważne muszą spełniać co najmniej założenia przyjęte w postępowaniu. Zamawiający dopuszcza możliwość zaproponowania rozwiązań równoważnych w stosunku do opisanych, z zastosowaniem tych samych standardów technicznych i jakościowych niezbędnych do prawidłowego funkcjonowania przedmiotu zamówienia.

Poprzez pojęcie rozwiązań równoważnych należy rozumieć rozwiązania zapewniające uzyskanie parametrów technicznych, jakościowych i użytkowych nie gorszych niż założone w opisie przedmiotu zamówienia. Wykonawca, który powołuje się na rozwiązania równoważne do rozwiązań opisywanych przez Zamawiającego, zobowiązany jest wykazać, że oferowany przez niego przedmiot zamówienia spełnia wymagania określone przez Zamawiającego.

Tam, gdzie w opisie przedmiotu zamówienia został wskazany konkretny typ, znak towarowy, marka, producent, dostawca, patent, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczone przez konkretnego wykonawcę, Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych w stosunku do wskazanych w opisie przedmiotu zamówienia pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych od założonych w opisie oraz będą zgodne pod względem:

- charakteru użytkowego (tożsamość funkcji),
- parametrów technicznych (wytrzymałość, trwałość, dane techniczne),
- parametrów bezpieczeństwa użytkowania.