Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Dla zadania pn. **„Zwiększenie bezpieczeństwa na ataki w cyberprzestrzeni, poprzez wdrożenie mechanizmów i zakup sprzętu IT związanych z cyberbezpieczeństwem dla Gminy Wijewo”**

Część I: **„Opracowanie, wdrożenie i aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem oraz audyt SZBI i zgodności KRI” – nie objęta szacowaniem wartości zamówienia**

Część II: **„Szkolenia z zakresu cyberbezpieczeństwa podstawowe oraz specjalistyczne” – nie objęta szacowaniem wartości zamówienia**

Część III: **„Zakup, konfiguracja oraz utrzymanie urządzeń i oprogramowań z zakresu cyberbezpieczeństwa” – zakup sprzętu IT**

Część IV: **„Zakup, konfiguracja oraz utrzymanie urządzeń i oprogramowań z zakresu cyberbezpieczeństwa” – zakup agregatu prądotwórczego**

Ad. 1. - nie objęta szacowaniem wartości zamówienia

Część I: **„Opracowanie, wdrożenie i aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem oraz audyt SZBI i zgodności KRI” - nie objęta szacowaniem wartości zamówienia**

Przedmiotem zamówienia jest usługa polegająca na opracowaniu, wdrożeniu i aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem oraz audyt SZBI i zgodności KRI w Urzędzie Gminy Wijewo w ramach projektu grantowego „Cyberbezpieczny Samorząd” w zakresie zgodnym z regulaminem naboru Konkursu Grantowego dostępnym na stronie https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad oraz określonym w niniejszym szacowaniu wartości zamówienia.

Miejsce realizacji przedmiotu zamówienia: **Wijewo, powiat leszczyński, województwo wielkopolskie.**

Wykonanie usługi obejmuje następujące etapy:

1) **Aktualizacja, a w przypadku braku poszczególnych dokumentów opracowanie pełnej dokumentacji tworzącej SZBI i niezbędnych procedur zgodnie z wymaganiami KRI/ISO27001 dla Urzędu Gminy Wijewo, wdrożenie i przegląd SZBI**
2) **Audyt KRI, ksc i testy podatności w 2025 r. w Urzędzie Gminy Wijewo**
3) **Przegląd SZBI w roku 2025 dla Urzędu Gminy Wijewo**
4) **Końcowy audyt zgodności przeprowadzany przez uprawnionego (certyfikowanego) audytora wiodącego ISO27001 lub równoważne w Urzędzie Gminy Wijewo**

Opis poszczególnych zadań realizowanych w ramach zamówienia:

Aktualizacja, a w przypadku braku poszczególnych dokumentów opracowanie pełnej dokumentacji tworzącej SZBI i niezbędnych procedur zgodnie z wymaganiami KRI/ISO27001 lub równoważne dla Urzędu Gminy Wijewo, wdrożenie SZBI w Przegląd SZBI w roku 2025:

1) Opracowanie/aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) spełniającego wymagania norm rodziny ISO 27000 lub równoważne w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 lub równoważne oraz zaleceniami aktualnych norm PN-ISO/IEC 27002 lub równoważne, PN-ISO-27005 lub równoważne), ISO 22301 lub równoważne i ISO 31000 lub równoważne w zakresie zarządzania ryzykiem, ustawę o Krajowym Systemie Cyberbezpieczeństwa, dyrektywę NIS2 i Rozporządzenie Parlamentu Europejskiego RODO, ustawę o informatyzacji podmiotów realizujących zadania publiczne oraz przepisów wykonawczych. Dokumentacja musi zawierać wszystkie niezbędne polityki i procedury, dokumenty niezbędne do zarządzania bezpieczeństwem informacji, instrukcje, wzory dokumentów, metodologie zarządzania ryzykiem itd.

Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb Urzędu Gminy Wijewo dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm.

Celem wdrożenia jest zapewnienie wysokiego poziomu bezpieczeństwa informacji w Urzędzie Gminy Wijewo i spełnienie wymagań obowiązujących przepisami prawa.

2) Wdrożenie opracowanego Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Gminy Wijewo.

3) Wykonawca zobowiązany jest do udziału w końcowym audycie zgodności przeprowadzonym przez uprawnionego audytora wiodącego ISO27001 lub równoważne w Urzędzie Gminy Wijewo, który zostanie zlecony przez Zamawiającego **najpóźniej na początku w roku 2026.**

Zadaniem Wykonawcy będzie udzielanie wyjaśnień i konsultacji dotyczących wdrożonego SZBI oraz wprowadzenie ewentualnych zmian lub poprawek w dokumentacji SZBI w przypadku wykazania takiej konieczności.

Audyt KRI, KSC i testy podatności w 2025 r. w Urzędzie Gminy Wijewo:

Audyt musi być dostosowany do wymagań rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zgodny z wymogami ustawy KSC.

Audyt musi być przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Minimalny zakres zadania:

Analiza wstępna stanu bezpieczeństwa informacji w Urzędzie Gminy Wijewo w zakresie objętym audytem:

- Identyfikacja obowiązujących wymagań, ocena istniejących systemów i procedur,
- Zebranie wstępnych odpowiedzi i dowodów audytowych,

- Rekomendacje dotyczące działań naprawczych i usprawnień,
- Raport z audytu,
- Wsparcie w ewentualnym opracowaniu i dostosowaniu dokumentacji i procedur obowiązujących w Urzędzie Gminy Wijewo,
- Przeprowadzenie testów podatności w Urzędzie Gminy Wijewo.

Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI).

Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI)/Krajowym Systemie Cyberbezpieczeństwa (KSC).

Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących umożliwiających minimalizację zidentyfikowanych ryzyk.

Wsparcie po audytowe, które polegać ma m.in. na udzielaniu informacji na temat audytowanych elementów wynikających z raportu, wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w Urzędzie Gminy Wijewo.

Audyt musi być wykonany przez osoby **uprawnione przepisami prawa**.

Wyniki audytu będą podstawą dalszych prac w Urzędzie Gminy Wijewo. Z przeprowadzonego audytu w Urzędzie Gminy Wykonawca opracuje i przedłoży Zamawiającemu raport w wersji papierowej – w 3 egz. i elektronicznej – 1 egz. Raport musi zawierać również wyniki sprawdzonych zagadnień określonych w ankiecie Dojrzałości Cyberbezpieczeństwa. Raport z audytu powinien być podpisany przez audytora opracowującego audyt (podpis kwalifikowalny lub własnoręczny w przypadku przedłożenia wersji papierowej). Zamawiający zastrzega prawo do wniesienia uwag do przedłożonej dokumentacji, a Wykonawca zobowiązuje się do jej skorygowania i uwzględnienia wniesionych uwag.

Przegląd SZBI w roku 2025 dla Urzędu Gminy Wijewo

Aktualizacja przygotowanej w 2025 r. dokumentacji SZBI, dostosowanie dokumentów do aktualnych wymagań.
Przegląd SZBI musi obejmować co najmniej:
- Sprawdzenie aktualności SZBI pod względem prawnym,
- Analizę ryzyka,
- Sprawdzenie funkcjonalności SZBI - dostosowania do Urzędu Gminy Wijewo,
- Ocena obecnego stanu Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Wijewo,
- Analiza zgodności z wymaganiami ISO 27001 lub równoważne i ISO 27002 lub równoważne,
- Identyfikacja luk i potencjalnych zagrożeń,

- Raport z wykonanych prac zawierający niezgodności oraz rekomendacje.

Wykonawca przeprowadzi przy udziale przedstawicieli Zamawiającego udokumentowanie analizy ryzyka, w tym opracowanie i wdrożenie metodyk zarządzania ryzykiem. Wskazanie obszarów wymagających dostosowania i/lub doskonalenia adekwatnie do przeprowadzonej analizy ryzyka oraz wymagane do wdrożenia zabezpieczenia. Wynikiem wdrożenia ma być zwiększenie cyberbezpieczeństwa, wprowadzenie i udokumentowanie Systemów Zarządzania Bezpieczeństwem Informacji, które będą wykorzystywane w Urzędzie Gminy Wijewo oraz pozwolą zapewnić zgodność podczas audytu końcowego w jednostce. Opracowana polityka, procedury, itp. muszą realnie odnosić się do procesów funkcjonujących w Urzędzie Gminy Wijewo.

Zamawiający oczekuje, że opracowane dokumenty będą napisane w języku polskim oraz zwięźle, językiem zrozumiałym dla osób nieposiadających wysokiego przygotowania z zakresu bezpieczeństwa informacji.

Jednocześnie Zamawiający zastrzega, że wszelkie błędy w przygotowanej dokumentacji świadczące o tym, że dokumentacja została przeniesiona z innej organizacji / jednostki będą podstawą do odrzucenia dokumentów do poprawy, bez ich dalszej analizy ze strony Zamawiającego.

<u>Końcowy audyt zgodności przeprowadzany przez uprawnionego (certyfikowanego) audytora wiodącego ISO27001 lub równoważne w Urzędzie Gminy Wijewo:</u>

Wykonawca zobowiązany jest do opracowania audytu końcowego, który jest warunkiem prawidłowego rozliczenia projektu pn. „Zwiększenie bezpieczeństwa na ataki w cyberprzestrzeni, poprzez wdrożenie mechanizmów i zakup sprzętu IT związanych z cyberbezpieczeństwem dla Gminy Wijewo".

Wykonawca jest zobowiązany do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z zapisami w § 20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247), zwanego dalej „rozporządzeniem KRI", zgodnie z poniższymi warunkami:

1) zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie JST obejmie zgodność z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001 lub równoważne
2) raport z audytu zostanie podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST i dostarczony do Zamawiającego
3) audyt systemu bezpieczeństwa informacji wdrożonego w Urzędzie Gminy Wijewo zostanie przeprowadzony przez:

a) audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999)
lub
b) audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001 lub równoważne;

Przeprowadzenie audytu zgodności musi obejmować **co najmniej:**
- analizę końcową stanu bezpieczeństwa informacji w urzędzie w zakresie objętym audytem,
- identyfikację obowiązujących wymagań, ocena istniejących systemów i procedur
- zebranie końcowych odpowiedzi i dowodów audytowych
- wspólne zdefiniowanie rekomendowanych działań korygujących w zakresie objętym audytem, rekomendacje dotyczące działań naprawczych i usprawnień
- opracowanie raportu z audytu,
- wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w Urzędzie Gminy Wijewo.

Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI).

Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC).

Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących.

Wsparcie poaudytowe, które polegać ma m.in. na: **udzielanie informacji na temat audytowanych elementów wynikających z raportu.**

Audyt musi być wykonany przez osoby uprawnione przepisami prawa.

W ramach zamówienia Wykonawca zobowiązany jest do opracowana **„Ankiety dojrzałości Cyberbezpieczeństwa”** na podstawie opracowanej ankiety przed realizacją projektu.
Ankieta jest załącznikiem nr 6 Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych) do regulaminu konkursu grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021 – 2027 (FERC).

UWAGA: Zamawiający zastrzega możliwość nieznacznej zmiany liczby osób zatrudnionych i użytkujących systemy na poszczególnych stanowiskach.

Warunkiem przeprowadzenia audytu jest dokonanie wizji lokalnej w miejscu wskazanym przez Zamawiającego. **Forma zdalna nie jest dopuszczalna.**

Celem przedsięwzięcia jest stworzenie kompleksowej strategii informatyzacji Urzędu Gminy Wijewo, gwarantującej najwyższy poziom bezpieczeństwa danych oraz pełną zgodność z obowiązującymi przepisami, w szczególności:

1. Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024. Poz.773),
2. Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.z 2024 r. poz. 1077 z późn. zm.)
3. Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz.307),
4. Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (tzw. Dyrektywa NIS 2).

Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb Urzędu Gminy Wijewo kompletne dokumentacje Systemu Zarządzania Bezpieczeństwem Informacji zgodne w/w wymaganiami, założeniami i normami.

UWAGA!!!

Akceptowane certyfikaty to w szczególności: Audytor wewnętrzny i zewnętrzny normy PN-ISO/ IEC 27001, CISA, CIA oraz równoważne poświadczenie / certyfikat z zakresu cyberbezpieczeństwa.

Oznaczenie wg Wspólnego Słownika Zamówień:

72800000-8 – Usługi audytu komputerowego i testowania komputerów

Inne informacje związane z przedmiotem zamówienia:

1) Termin realizacji zamówienia:

a) Audyt wstępny zgodności KRI w Urzędzie Gminy Wijewo – **do 2 miesięcy od dnia zawarcia umowy,**
b) Aktualizacja posiadanej dokumentacji SZBI w Urzędzie Gminy Wijewo oraz opracowanie i wdrożenie SZBI w Urzędzie Gminy Wijewo – **do 5 miesięcy od dnia zawarcia umowy,**
c) Wykonanie audytu końcowego zgodności KRI w Urzędzie Gminy Wijewo – **najpóźniej do dnia 28 lutego 2026 r.**

Zamawiający przewiduje przedłużenie terminu realizacji danej części zamówienia, w wyniku przedstawienia przez Wykonawcę w formie pisemnej wniosku o przedłużenie terminu realizacji danej części zamówienia. Wniosek należy złożyć nie później niż 1 miesiąc przed planowanym zakończeniem realizacji umowy. Zamawiający może udzielić Wykonawcy zgody na przedłużenie realizacji zamówienia, jednak ostatecznym terminem realizacji zamówienia jest dzień 28 luty 2026 r.

Przelew w terminie 21 dni od dnia otrzymania prawidłowo wystawionej faktury VAT / rachunku potwierdzonej protokołem końcowym odbioru należycie wykonanych usług. Zamawiający dopuszcza wystawienie faktury po każdym zakończonym etapie.

Opis warunków udziału w postępowaniu oraz opis sposobu dokonywania oceny spełnienia tych warunków:

O udzielenie niniejszego zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki udziału w postępowaniu dotyczące:

1) Zdolności do występowania w obrocie gospodarczym
Zamawiający nie wyznacza szczegółowego warunku w tym zakresie;
2) Uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej
Zamawiający nie wyznacza szczegółowego warunku w tym zakresie;
3) Sytuacji ekonomicznej lub finansowej
Zamawiający nie wyznacza szczegółowego warunku w tym zakresie;
4) Zdolności technicznej lub zawodowej:
O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają łącznie następujące warunki:

1. W okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy, w tym terminie, wykonali usługi opracowania dokumentacji systemu zarządzania bezpieczeństwem informacji wg normy PN-EN ISO / IEC 27001 lub równoważne w co najmniej dwóch instytucjach. Decyduje data odbioru zamówienia. Pod pojęciem opracowania rozumie się także aktualizację istniejącej w organizacji dokumentacji SZBI.
2. Dysponują i przeznaczą do realizacji zamówienia co najmniej jedną osobę będącą:

a) Audytorem zewnętrznym posiadającym co najmniej jeden z aktualnych certyfikatów, o których mowa w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, lub
b) Audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO / IEC 27001 lub równoważne.

Zamawiający wymaga, aby audytor wskazany do wykonania usługi, w okresie trzech ostatnich lat przed upływem terminu składania ofert, brał czynny udział w co najmniej dwóch usługach polegających na opracowaniu systemu zarządzania bezpieczeństwem informacji. Decyduje data odbioru zamówienia. Pod pojęciem opracowania rozumie się także aktualizację istniejącej w organizacji dokumentacji SZBI.

Zamawiający dopuszcza możliwość wykonania usługi przez inne osoby niż wskazane w ofercie, pod warunkiem, że osoby te będą spełniały warunki udziału w postępowaniu określone w szacowaniu wartości zamówienia. Potrzeba zmiany osoby skierowanej do wykonania zamówienia musi zostać zgłoszona Zamawiającemu wraz z uzasadnieniem, najpóźniej 3 dni robocze przed datą rozpoczęcia usługi, a w przypadkach losowych w ciągu 3 dni roboczych od wystąpienia zdarzenia uniemożliwiającego wykonanie lub ukończenie wykonania usługi, w formie pisemnej. Zmiana wymaga zatwierdzenia przez Zamawiającego.

Ocena spełniania warunków w postępowaniu odbędzie się na podstawie przedłożonych dokumentów poprzez stwierdzenie: *spełnia/ nie spełnia.*

Ad. 2.

Część II: **„Szkolenia z zakresu cyberbezpieczeństwa podstawowe oraz specjalistyczne” - nie objęta szacowaniem wartości zamówienia**

Szkolenie dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001:

Przeprowadzenie szkoleń dla pracowników i kierownictwa Urzędu Gminy Wijewo z SZBI oraz podstaw ISO 27001 lub równoważne – **szkolenie stacjonarne** dla ok. 23-25 osób, w podziałach: szkolenie podstawowe na min. 2 grupy, rozłożone na 2 dni robocze (jedna grupa = jeden dzień szkolenia), czas trwania **co najmniej ok. min. 5 godzin/każda grupa.** Ponadto jedno szkolenie dla kadry zarządzającej ok. 7 osób, szkolenie w przedmiocie zaawanasowanych zagadnień bezpieczeństwa informatycznego takich jak np. zarządzanie bezpieczeństwem informatycznym, testowanie penetracyjne, reagowania incydenty bezpieczeństwa informatycznego - czas trwania **co najmniej ok. min. 5 godzin zegarowych**. ***Szkolenia stacjonarne, miejsce szkolenia sala posiedzeń w Urzędzie Gminy Wijewo (Wijewo, ul. Parkowa 1). Szkolenie zorganizowane w przedziale godzinowym 8.00 – 14.00, od poniedziałku do piątku.***

Przygotowane przez Wykonawcę materiały szkoleniowe oraz certyfikaty muszą zostać oznaczone informacją o finansowaniu przedmiotu zamówienia ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), zgodnie z Regulaminem Konkursu

Grantowego „Cyberbezpieczny Samorząd”. (zasady zostały określone w dokumencie pn. „Podręcznik wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji” zamieszczonego na stronie internetowej www.funduszeeuropejskie.gov.pl).

W ramach organizacji szkolenia Wykonawca zapewni właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikom (zasady zostały określone w dokumencie pn. „Podręcznik wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji” zamieszczonego na stronie internetowej
www.funduszeeuropejskie.gov.pl).

We wszystkich częściach zamówienia muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępność dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn W sytuacji, kiedy szkolenia będą prowadzone w formie stacjonarnej wykonawca będzie musiał zapewnić materiał szkoleniowy z większym rozmiarem czcionki (w zależności od potrzeb uczestników szkolenia). W ramach grup szkoleniowych przewidziana jest równa dostępność dla kobiet i mężczyzn oraz osób niepełnosprawnych. Opracowane dokumentacje będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści.

Podczas szkolenia Zamawiający będzie przeprowadzał dokumentację fotograficzną w celach promocyjnych. Wykonawca zawierając umowę z Zamawiającym wyraża zgodę na ich publikowanie na stronie internetowej oraz w mediach społecznościowych Zamawiającego, jak również na ich przetwarzanie w ramach dokumentacji organizacji szkoleń w ramach projektu.

Program szkolenia przygotowuje Wykonawca, program ma być dostosowany do tematyki szkolenia oraz przygotowany pod kątem uczestników szkolenia tj. pracownicy Urzędu Gminy Wijewo.

Program szkolenia musi uzyskać akceptację Zamawiającego.

Szkolenie zakończone uzyskaniem zaświadczenia o udziale w szkoleniu dla każdego pracownika/kierownika uczestniczącego w szkoleniu.

Szkolenie musi posiadać wysoką jakość merytoryczną przygotowanego scenariusza. Scenariusz szkolenia musi zostać opracowany we współpracy z ekspertem bezpieczeństwa IT posiadającym certyfikat Lead Auditor 27001.

Wymogi dotyczące oferenta:

- Oferent powinien dysponować minimum jednym trenerem posiadającymi ważny certyfikat CISSP zatrudnionym w oparciu o umowę o pracę lub inny stosunek zobowiązaniowy

Data graniczna wykonania szkoleń **– 31 grudnia 2025 roku.**

7. Termin realizacji : – uruchomienia usługi : **14 dni od daty zawarcia umowy ;**
– zakończenie szkoleń :do dnia **31 grudnia 2025 r.**

Zamawiający przewiduje przedłużenie terminu realizacji danej części zamówienia, w wyniku przedstawienia przez Wykonawcę w formie pisemnej wniosku o przedłużenie terminu realizacji danej części zamówienia. Wniosek należy złożyć nie później niż 1 miesiąc przed planowanym zakończeniem realizacji umowy. Zamawiający może udzielić Wykonawcy zgody na przedłużenie realizacji zamówienia, jednak ostatecznym terminem realizacji zamówienia jest dzień 28 luty 2026 r.

Zamawiający nie ponosi kosztów dojazdu, zakwaterowania oraz wyżywienia wykonawcy, a także dodatkowych kosztów związanych z przygotowaniem materiałów szkoleniowych i promocyjnych.

Obowiązkiem Zamawiającego będzie zapewnienie:
1. Nieodpłatne udostępnienie lokalu (sali szkoleniowej dla wymaganej liczby uczestników) z dostępem do Internetu oraz energii elektrycznej.
2. Rekrutacji osób biorących udział w szkoleniach oraz ustalenie składu grup – w przypadku nieobecności uczestnika na zajęciach prowadzonych w ramach jego grupy szkoleniowej, uczestnik może dołączyć do innej grupy.

Ad. 3

Część III: **„Zakup, konfiguracja oraz utrzymanie urządzeń i oprogramowań z zakresu cyberbezpieczeństwa" – zakup sprzętu IT**

ZESTAWIENIE + specyfikacje minimalne

1. **Serwer**

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max. 2U umożliwiającą instalację min. 12 dysków 3,5" z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Płyta główna	Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory min. ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 44000 punktów w teście PassMark dostępnym na stronie www.cpubenchmark.net dla dwóch procesorów.
RAM	Min. 64 GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Zabezpieczenia pamięci RAM	Fault Resilient Memory (FRM), Self Healing, Adaptive Double Device Data Correction (ADDDC), Memory Health Check, Memory Page Retire
Interfejsy sieciowe/FC/SAS	Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz cztery interfejsy sieciowe 10Gb Ethernet w standardzie BaseT nie zajmujące regularnych gniazd PCI Express. Zainstalowana dodatkowa karta sieciowa PCI Express wyposażona w dwa interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28
Dyski twarde	Możliwość instalacji dysków SAS/SATA Zainstalowane trzy dyski hot-plug SSD SATA o pojemności min. 960GB, dopuszczalna liczba zapisów min. 1DWPD Zainstalowane dwa dyski hot-plug HDD SATA o pojemności min. 4TB,

	Zainstalowane dwa dyski M.2 SATA o pojemności min. 480 GB z możliwością konfiguracji RAID 1
Kontroler RAID/HBA	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60.
Wbudowane porty	min. 4 porty USB, w tym minimum 1 port USB 3.0, 2 porty VGA, min. 1 port sieciowy BaseT dedykowany do zarządzania
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Wentylatory	Redundantne
Zasilacze	Min. dwa zasilacze Hot-Plug, każdy o mocy maksymalnie 1100W, klasa sprawności Titanium. Do serwera należy dołączyć 2 kable zasilające C13-C14, każdy o długości min. 2 metrów.
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela przedniego zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą TPM 2.0 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. Możliwość integracji z RSA SecurID
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów

	• wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232. • możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • możliwość monitorowania z jednej konsoli min. 100 serwerów fizycznych • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. • Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej 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 lub WIFI. Karta powinna posiadać możliwość rozszerzenia o takie funkcjonalnosci jak: • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe

	• kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • Automatyczne odświeżanie certyfikatów SSL • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe • monitorowanie przepływu powietrza na bieżąco
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostały czas gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • 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, informacja 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 podstwie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w opraciu 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 zarzadzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
System Operacyjny	• Licencja na serwerowy system operacyjny (zwany dalej SSO) Windows Server 2022 Standard, pokrywająca wszystkie fizyczne rdzenie procesora, umożliwiająca uruchomienie minimum 2 wirtualnych wystąpień SSO. • Licencje dostępowe do SSO dla min. 50 użytkowników • Licencje dostępowe do SSO umożliwiające zdalny dostęp na serwer w ilości min. 5 sztuk
System bazodanowy	• Licencja na serwerowy system bazodanowy Microsoft SQL Server 2022 Standard • Licencje dostępowe do serwerowego systemu bazodanowego dla min. 10 użytkowników

Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64.
Normy Środowiskowe	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 potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - ***Wykonawca złoży dokument potwierdzający spełnianie*** **wymogu.** Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych **w postaci oświadczenia producenta serwera** (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr - ***Wykonawca złoży dokument potwierdzający spełnianie*** **wymogu.**
Warunki gwarancji	Zamawiający wymaga min. 60 miesięcy gwarancji producenta i możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami:

	telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. 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. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Licencje na wbudowane oprogramowanie: min. 2 lata.

Wymagane przeszkolenie pracowników z obsługi instalowanego urządzenia.

2. UPS do serwera

Na wyjściu	
Moc wyjściowa	1.2kW / 1,5kVA
Topologia	Line Interactive
Typ przebiegu	Sinusoida
Złącza wyjściowe	(8) IEC 320 C13 (Zasilanie zapasowe)
Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą)	50/60Hz +/- 3 Hz
Inne napięcia wyjściowe	208, 220, 240
Czas przełączania	6ms typowo (max. 10ms)
Na wejściu	
Długość przewodu zasilania	1.83 m
Częstotliwość wejściowa	50/60 Hz +/-3 Hz (automatyczne wykrywanie)
Zakres napięcia wejściowego w trybie podstawowym	151 - 302V
Akumulatory i czas podtrzymania	
Typ akumulatora	Bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny
Typowy czas ładowania	3 godziny
Czas podtrzymania przy obciążeniu 100%	5,4 min
Czas podtrzymania przy obciążeniu 50%	17,2 min
Możliwość podłączenia do 10 zewnętrznych modułów akumulatorowych	TAK
Panel sterowania	Wyświetlacz statusu LED ze wskaźnikiem pracy online: Zasilanie akumulatorowe: Wskaźniki Wymień baterię i Przeciążenie, Wielofunkcyjna konsola sterownicza i informacyjna LCD
Alarm dźwiękowy	Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia
Awaryjny wyłącznik zasilania (EPO)	TAK

Ochrona przed przepięciami i filtracja	
Klasa energetyczna sprzętu przeciwprzepięciowego	645J
Certyfikaty i zgodność z normami	
Potwierdzenia zgodności	CE, EAC, EN/IEC 62040-1, EN/IEC 62040-2, RCM, VDE
Okres gwarancji	Gwarancja zgodna z okresem udzielonym przez producenta
Dodatkowe informacje	Możliwość zastosowania w wersji wolnostojącej i do montażu w szafie przemysłowej Możliwość zimnego startu
Ilość	1 sztuka

3. UPS-y do komputerów

Moc pozorna	750 VA
Moc skuteczna	410 W
Napięcie wyjściowe	230 V
Napięcie wejściowe	230 V
Gniazdo wejściowe	CEE 7/7 (Kompatybilne z Typ E i Typ F)
Długość przewodu	1.2 m
Złącza	3 x Typ E CEE 7/5 (Podtrzymanie/ochrona) RJ-45 In/Out (Ochrona) USB-B (Zarządzanie)
Topologia	Line-Interactive
Typ przebiegu	Schodkowa aproksymacja sinusoidy
Czas przełączania	6 ms (Typowe) 10 ms (Maksymalne)
Akumulator	Bezobsługowy kwasowo-ołowiowy
Typowy czas ładowania	8 godzin
Czas podtrzymania (50%)	7 min
Czas podtrzymania (100%)	0.71 min
Bezpieczeństwo	Podtrzymanie zasilania Ochrona przeciwprzepięciowa Automatyczna regulacja napięcia (AVR)
Zarządzanie	Oprogramowanie PowerChute
Wymiary	Wysokość – 16 cm Szerokość – 12 cm Głębokość – 36 cm Waga – 5.40 kg
Dodatkowe informacje	Zimny start

	Alarmy dźwiękowe
Gwarancja	Gwarancja zgodna z okresem udzielonym przez producenta
Ilość	26 sztuk

4. **Switch zarządzany**

Wbudowana pamięć	96K SRAM
Ethernet	(5) portów Ethernet 10/100/1000; Przełącznik Atheros AR8327
SFP	Jedna klatka Gigabit Ethernet SFP z obsługa DDMI (mini-GBIC; moduł SFP nie jest dołączony)
Diody LED	Zasilanie, aktywność NAND, 5 diod LED aktywność Ethernet
Dodatki	Sprzętowy watchdog
Opcje zasilania	PoE: 8-30 V DC na Ether1 (bez 802.3af) Gniazdo 8-30 V DC
Wymiary i waga	113 mm x 138 mm x 29 mm. Bez opakowania i zasilacza: 212 g
Zużycie energii elektrycznej	Do 6 W
Zakres temperatury pracy	Od -25°C do 65°C
System operacyjny	MikroTik Swos
Ilość	10 sztuk
Gwarancja	Gwarancja zgodna z okresem udzielonym przez producenta

5. **Oprogramowanie do zarządzania i inwentaryzacji sprzętu i oprogramowania**

Funkcje	Inwentaryzacja zasobów IT (sprzętów oraz oprogramowania) Automatyczny audyt sprzętu Generowanie protokołów przekazania, zwrotu i likwidacji Wbudowany skaner sieci Tworzenie własnych typów zasobów Definiowanie atrybutów zasobów Kreator formularzy zasobów Wydruk kodów kreskowych Tworzenie relacji pomiędzy zasobami Historia relacji

	Historia zmian wartości atrybutów Kreator protokołów (np. przekazania, zwrotu, likwidacji) Repozytorium plików (np. faktura, karta gwarancyjna) Integracja z modułem ServiceDesk (podgląd użytkownika w posiadane zasoby) Import danych zewnętrznych Kreator raportów (wg typów zasobów, użytkowników, lokalizacji) Zarządzanie zasobami poprzez reguły (warunki oraz akcje) Powiadomienia mailowe (nowy zasób, likwidacja)

Inne informacje:

Wszystkie ewentualne wskazane w dokumentacji szacowania znaki towarowe, patenty, nazwy producentów, pochodne lub źródło albo wskazany szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę są podane jedynie przykładowo i Zamawiający dopuszcza zastosowanie innych materiałów o równoważnych parametrach jakościowych. Zamawiający dopuszcza oferowanie materiałów lub rozwiązań równoważnych, pod warunkiem, że zagwarantują one wykonanie zamówienia w zgodzie z treścią szacowania oraz zapewnią uzyskanie parametrów technicznych i użytkowych nie gorszych od założonych w wyżej wymienionych dokumentach. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji, na wykonawcy ciąży obowiązek każdorazowego przedłożenia Zamawiającemu stosownych dokumentów, stwierdzających, że proponowane materiały, dostawy i technologia zamiennie spełniają (nie są gorsze) warunki / parametry techniczne i użytkowe zawarte w dokumentacji postępowania. Obowiązek udowodnienia równoważności powiązań technicznych i użytkowych leży wyłącznie po stronie Wykonawcy.

UWAGA!!!!

Wszelkie koszty naprawy, w tym koszt transportu, ubezpieczenia na czas transportu, instalacji i ponownego uruchomienia ponosi Wykonawca.

Serwis gwarancyjny możliwy będzie do świadczenia u Zamawiającego z możliwością naprawy u Wykonawcy w sytuacjach, kiedy naprawa u Zamawiającego okaże się niemożliwa.

Ad. 4

Część IV: **„Zakup, konfiguracja oraz utrzymanie urządzeń i oprogramowań z zakresu cyberbezpieczeństwa" – zakup agregatu prądotwórczego**

1. **Agregat prądotwórczy do serwera**

Dane techniczne silnika	Silnik wysokoprężny, 4-suwowy Ilość obrotów 3000 Napędzany olejem napędowym (diesel) Chłodzony powietrzem Wtrysk bezpośredni (pompowtryskiwacz) Papierowy filtr powietrza Filtr paliwa umieszczony pod zbiornikiem Filtr oleju metalowy, wielorazowy Rozrząd zaworowy napędzany kołem zębatym Silnik z pompą olejową (wymuszone smarowanie) Rozrusznik elektryczny o mocy min. 800W Czujnik poziomu oleju Czujnik ciśnienia oleju Pojemność miski olejowej 1.60L Zawór elektromagnetyczny sterowany pojedynczym elektromagnesem
Specyfikacja prądnicy	Moc maksymalna - 7.6 kW (9,5 kVA) Moc znamionowa - 7.0 kW (8.7 kVA) Uzwojenia w 100% z miedzi Napięcie wyjściowe 230V/12V Zabezpieczenie 1xC32 Czysta sinusoida (AVR 2%) Regulator napięcia AVR Samowzbudna
Parametry obudowy	Wymiary: 70(wys.) × 52(szer.) x 92(di) cm, 160kg Wzmocniona konstrukcja stalowa Zbiornik paliwa o pojemności 12.5L Łatwy dostęp do prac serwisowych Koła transportowe oraz uchwyty transportowe Hak do udźwigu Dostęp chroniony zamkami na kluczyki
Warunki gwarancji	Gwarancja zgodna z okresem udzielonym przez producenta.
Montaż	**Wykonawca zapewnia profesjonalne zainstalowanie i podłączenie generatora w miejscu wskazanym przez Zamawiającego wraz z przeprowadzeniem próbnego**

	rozruchu, który ma być objęty gwarancją prawidłowego funkcjonowania agregatu.
Dodatkowe elementy	Ponadto Zamawiający wymaga w ramach zakupu agregatu prądotwórczego **dostarczenie samoczynnego załączenia rezerwy (Automatyka) z blokadą mechaniczną.** Układ samoczynnego załączenia rezerwy. Dzięki temu urządzeniu agregat jest w trybie „czuwania" i jest nieustannie gotowy do automatycznego uruchomienia się w momencie zaniku prądu w sieci. Podczas pracy w trybie „czuwania" akumulator w agregacie jest na podtrzymaniu a więc nie ma obawy że akumulator się rozładuje
Ilość	1 sztuka

Dostawca w ramach zamówienia zobowiązany będzie do uruchomienia dostarczonego sprzętu i przeprowadzenia jego skuteczności działania. Wymagane przeszkolenie pracowników z obsługi instalowanych urządzeń.

UWAGA!!!!

Wszelkie koszty naprawy, w tym koszt transportu, ubezpieczenia na czas transportu, instalacji i ponownego uruchomienia ponosi Wykonawca.

Serwis gwarancyjny możliwy będzie do świadczenia u Zamawiającego z możliwością naprawy u Wykonawcy w sytuacjach, kiedy naprawa u Zamawiającego okaże się niemożliwa.

Inne informacje:

Wszystkie ewentualne wskazane w dokumentacji szacowania znaki towarowe, patenty, nazwy producentów, pochodne lub źródło albo wskazany szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę są podane jedynie przykładowo i Zamawiający dopuszcza zastosowanie innych materiałów o równoważnych parametrach jakościowych. Zamawiający dopuszcza oferowanie materiałów lub rozwiązań równoważnych, pod warunkiem, że zagwarantują one wykonanie zamówienia w zgodzie z treścią szacowania oraz zapewnią uzyskanie parametrów technicznych i użytkowych nie gorszych od założonych w wyżej wymienionych dokumentach. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji, na wykonawcy ciąży obowiązek każdorazowego przedłożenia Zamawiającemu stosownych dokumentów, stwierdzających, że proponowane materiały, dostawy i technologia zamiennie spełniają (nie są gorsze) warunki / parametry techniczne i użytkowe zawarte w dokumentacji postępowania. Obowiązek udowodnienia równoważności powiązań technicznych i użytkowych leży wyłącznie po stronie Wykonawcy.