



Numer sprawy: ZP.271.13.2025

Przasnysz, dnia 9 czerwca 2025 r.

Szczegółowy Opis Przedmiotu Zamówienia

na postępowanie pn. „Dostawy i usługi związane z realizacją projektu w ramach grantu „Cyberbezpieczny Samorząd” (2 części)”

wraz ze wskazaniem wymagań jakościowych odnoszących się do głównych elementów składających się na przedmiot zamówienia



Spis treści

1. Zestawienie ilościowe.3
2. Zasada równoważności rozwiązań i neutralności technologicznej.4
3. Przedmiot zamówienia dla części nr 1.12
- 3.1. Wymagania ogólne.12
- 3.2. Zakup usług aktualizacji i wdrożenia SZBI.14
- 3.3. Zakup usług przeprowadzenia audytu zgodności KRI.19
- 3.4. Zakup usług szkolenia pracowników z cyberbezpieczeństwa (100 osób).23
4. Przedmiot zamówienia dla części nr 2.26
- 4.1. Wymagania ogólne.26
- 4.2. Zakup serwera (1 szt.).27
- 4.3. Zakup NAS TYP A (2 szt.).30
- 4.4. Zakup NAS TYP B (1 szt.).31
- 4.5. Zakup przełączników sieciowych TYP A (4 szt.).32
- 4.6. Zakup przełączników sieciowych TYP B (3 szt.).33
- 4.7. Zakup przełączników sieciowych TYP C (12 szt.).33
- 4.8. Zakup UPS TYP A (2 szt.).34
- 4.9. Zakup UPS TYP B (54 szt.).34
- 4.10. Zakup usług backup w chmurze (1 szt.).35

1. Zestawienie ilościowe.

Część nr 1 – Przeprowadzenie audytów KRI oraz aktualizacja i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji dla urzędu wraz ze szkoleniami z cyberbezpieczeństwa.

Lp.	Nazwa	Ilość
1.	Zakup usług aktualizacji i wdrożenia SZBI	1 szt.
2.	Zakup usług przeprowadzenia audytu zgodności KRI	2 szt.
3.	Zakup usług szkolenia pracowników z cyberbezpieczeństwa	100 osób

Część nr 2 – Dostawa sprzętu i oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Zakup serwera	1 szt.
2.	Zakup NAS TYP A	2 szt.
3.	Zakup NAS TYP B	1 szt.
4.	Zakup przełączników sieciowych TYP A	4 szt.
5.	Zakup przełączników sieciowych TYP B	3 szt.
6.	Zakup przełączników sieciowych TYP C	12 szt.
7.	Zakup UPS TYP A	2 szt.
8.	Zakup UPS TYP B	54 szt.
9.	Zakup usług backup w chmurze	1 szt.

2. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanym w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może proponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznaczących różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt

o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

12. Za równoważną do normy ISO 9001 Zamawiający uzna normę, która dotyczy zarządzania jakością ustanawiając wymagania dla systemów zarządzania jakością w organizacjach w minimum następującym zakresie:

- a. Skupienie na użytkowniku – Podstawowym celem systemu zarządzania jakością jest zwiększenie satysfakcji użytkownika poprzez spełnianie jego wymagania oraz oczekiwania. Organizacja powinna monitorować potrzeby użytkowników i dostarczać produkty lub usługi, które je zaspokajają.
- b. Przywództwo – Wspieranie kierownictwa w zapewnianiu odpowiednich zasobów i wsparcia w procesach zarządzania jakością. Przywódcy powinni tworzyć środowisko, które wspiera zaangażowanie pracowników w poprawę jakości.
- c. Zaangażowanie ludzi – Organizacja powinna zapewnić, aby wszyscy pracownicy byli zaangażowani w realizację celów jakościowych. Kluczowym elementem jest angażowanie personelu w procesy poprawy jakości i podejmowanie działań na rzecz doskonalenia.
- d. Podejście procesowe – Norma podkreśla, że organizacja powinna zarządzać swoimi procesami w sposób spójny i skuteczny, traktując je jako powiązane ze sobą elementy systemu zarządzania jakością, które wspólnie prowadzą do osiągnięcia celów organizacji.
- e. Podejście systemowe do zarządzania – Organizacja powinna traktować system zarządzania jakością jako całość, złożoną z wzajemnie powiązanych elementów (np. procesów, zasobów, technologii), które muszą działać w harmonii, aby osiągnąć cele jakościowe.
- f. Ciągłe doskonalenie – dążenie do ciągłego doskonalenia procesów w organizacji. Ciągłe doskonalenie jest kluczowym elementem skutecznego zarządzania jakością i poprawy wyników.
- g. Podejście do podejmowania decyzji oparte na faktach – w procesie podejmowania decyzji organizacja powinna opierać się na danych i analizach, a nie na przypuszczeniach czy intuicji. Podejście to pozwala na bardziej precyzyjne i obiektywne decyzje.
- h. Relacje z dostawcami na zasadzie wzajemnych korzyści – tworzenie partnerskich relacji z dostawcami, które będą korzystne dla obu stron. Współpraca z dostawcami powinna być oparta na zaufaniu i dążeniu do wspólnych celów jakościowych.
- i. Zarządzanie ryzykiem – norma wymaga, aby organizacje identyfikowały, oceniały i zarządzały ryzykiem związanym z procesami oraz ich wpływem na zdolność organizacji do dostarczania produktów i usług o wymaganej jakości.
- j. Dokumentowanie systemu zarządzania jakością – Norma określa wymagania dotyczące dokumentowania systemu zarządzania jakością, w tym tworzenia polityki jakości, procedur, instrukcji roboczych oraz zapisów, które umożliwiają monitorowanie i weryfikację skuteczności systemu.

13. Za równoważną do normy ISO 50001 Zamawiający uzna normę, która dotyczy zarządzania energią w organizacjach w minimum następującym zakresie:

- a. Skupienie na poprawie efektywności energetycznej – Celem normy jest poprawa efektywności wykorzystania energii poprzez identyfikację obszarów, w których możliwe są oszczędności i usprawnienia w zarządzaniu energią.
- b. Zarządzanie cyklem życia energii – uwzględnia cały cykl życia energii, od planowania, poprzez wykorzystanie, aż po monitorowanie, ocenę i doskonalenie działań mających na celu zmniejszenie zużycia energii.
- c. Zintegrowane podejście z innymi systemami zarządzania – Norma jest zaprojektowana w sposób zgodny z innymi międzynarodowymi normami, co umożliwia integrację systemów zarządzania w organizacji.
- d. Podejście oparte na cyklu PDCA (Plan-Do-Check-Act) – opiera się na cyklu PDCA, który wspiera organizacje w procesie ciągłego doskonalenia zarządzania energią poprzez planowanie, wdrażanie, monitorowanie i działania korygujące.
- e. Zaangażowanie kierownictwa – Norma wymaga, aby najwyższe kierownictwo organizacji angażowało się w proces zarządzania energią, podejmując decyzje, dostarczając zasoby oraz ustalając cele i polityki energetyczne.
- f. Ustalenie polityki energetycznej – norma zachęca organizacje do opracowania polityki energetycznej, która definiuje kierunki działań, cele efektywności energetycznej oraz zobowiązania do ciągłego doskonalenia.
- g. Identyfikacja i ocena aspektów energetycznych – Norma wymaga przeprowadzenia analizy aspektów energetycznych, które mają istotny wpływ na zużycie energii i środowisko, oraz wdrożenia działań na rzecz ich poprawy.
- h. Monitorowanie, pomiar i analiza – nakłada obowiązek monitorowania i mierzenia zużycia energii oraz wydajności energetycznej organizacji. Organizacja powinna także stosować odpowiednie narzędzia do analizy wyników, identyfikacji możliwości poprawy oraz podejmowania działań korygujących.
- i. Zarządzanie ryzykiem i szansami – Norma podkreśla znaczenie identyfikacji ryzyk i szans związanych z zarządzaniem energią, a także działań na rzecz minimalizowania ryzyka i maksymalizowania możliwości poprawy efektywności energetycznej.
- j. Ciężar działań edukacyjnych i szkoleń – Norma wskazuje na konieczność zapewnienia odpowiedniego poziomu wiedzy i umiejętności w zakresie zarządzania energią dla wszystkich pracowników organizacji. Szkolenia i podnoszenie świadomości energetycznej są kluczowe dla skutecznego wdrażania polityki energetycznej.

14. Za równoważną do normy ISO 14001 Zamawiający uzna normę, która dotyczy systemów zarządzania środowiskowego w minimum następującym zakresie:

- a. Zarządzanie środowiskowe oparte na cyklu PDCA (Plan-Do-Check-Act) – norma opiera się na cyklu PDCA, który wspiera organizacje w systematycznym zarządzaniu i doskonaleniu ich działań na rzecz ochrony środowiska. Proces obejmuje planowanie, wdrażanie, monitorowanie oraz podejmowanie działań korygujących.
- b. Zobowiązanie organizacji do ochrony środowiska – Norma wymaga, aby organizacja była zobowiązana do minimalizowania negatywnego wpływu na środowisko. To zobowiązanie powinno być wyrażone poprzez politykę środowiskową, która wskazuje na cele ochrony środowiska.

- c. Identyfikacja aspektów środowiskowych – Organizacja musi identyfikować i oceniać aspekty środowiskowe związane z jej działalnością, produktami i usługami. Ocena powinna uwzględniać wpływ na środowisko, zarówno w zakresie zużycia zasobów, jak i wytwarzania odpadów oraz emisji.
 - d. Zgodność z przepisami prawnymi i innymi wymaganiami – norma wymaga, aby organizacja przestrzegała obowiązujących przepisów prawnych dotyczących ochrony środowiska oraz innych zobowiązań, które organizacja uzna za stosowne (np. normy branżowe).
 - e. Cele środowiskowe i planowanie działań – Organizacja musi wyznaczać mierzalne cele środowiskowe i opracować plany działań, które pozwolą osiągnąć te cele. Cele te powinny być zgodne z polityką środowiskową i uwzględniać aspekt środowiskowy w całym cyklu życia produktów i usług.
 - f. Zaangażowanie kierownictwa – zaangażowanie najwyższego kierownictwa w wdrażanie systemu zarządzania środowiskowego. Kierownictwo powinno zapewnić zasoby, nadzór i wspierać działania na rzecz ochrony środowiska.
 - g. Zarządzanie ryzykiem środowiskowym – Norma podkreśla konieczność identyfikacji i oceny ryzyk środowiskowych związanych z działalnością organizacji. Organizacja powinna podejmować działania na rzecz minimalizowania ryzyk, a także wdrażać procedury zapobiegania i reagowania na sytuacje kryzysowe.
 - h. Monitorowanie, pomiar i analiza wyników – Organizacja jest zobowiązana do monitorowania i mierzenia skuteczności swoich działań środowiskowych. Obejmuje to ocenę wpływu działań na środowisko, skuteczność realizacji celów oraz identyfikację obszarów do poprawy.
 - i. Działania korygujące i zapobiegawcze – norma wymaga, aby organizacja wdrażała procedury podejmowania działań korygujących w przypadku niezgodności oraz działań zapobiegawczych, aby uniknąć powtarzania się problemów środowiskowych w przyszłości.
 - j. Ciągłe doskonalenie systemu zarządzania środowiskowego – Podstawowym celem normy jest dążenie do ciągłego doskonalenia systemu zarządzania środowiskowego. Organizacja powinna regularnie przeglądać i aktualizować swoje cele, polityki i procesy, aby dostosować je do zmieniających się warunków środowiskowych oraz wymagań prawnych.
15. Za równoważną do normy ISO 27001 Zamawiający uzna normę, która określa standard zarządzania bezpieczeństwem informacji w minimum następującym zakresie:
- a. Zarządzanie ryzykiem – norma stosuje podejście oparte na zarządzaniu ryzykiem. Organizacja musi przeprowadzać ocenę ryzyka dla bezpieczeństwa informacji i podejmować odpowiednie środki w celu zarządzania tym ryzykiem.
 - b. Ochrona informacji – Norma zapewnia, że organizacja identyfikuje, ocenia i zabezpiecza informacje, w tym dane osobowe, finansowe, techniczne, i inne zasoby przed zagrożeniami.
 - c. Ciągłość działania – norma kładzie nacisk na ciągłość działania w przypadku awarii systemów, katastrof naturalnych, ataków cybernetycznych itp. Organizacje muszą przygotować plany awaryjne i procedury odzyskiwania danych.
 - d. Zaangażowanie kierownictwa – Norma wymaga aktywnego zaangażowania najwyższego kierownictwa w procesie zarządzania bezpieczeństwem informacji.

- e. Ciągłe doskonalenie – norma promuje ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji, aby dostosować go do zmieniających się zagrożeń i wymagań.
 - f. Polityki bezpieczeństwa informacji – norma określa, że organizacja musi opracować i wdrożyć formalne polityki bezpieczeństwa informacji, które są zgodne z jej celami biznesowymi i wymaganiami regulacyjnymi.
 - g. Szkolenia i świadomość pracowników – norma kładzie nacisk na edukację i szkolenia pracowników w zakresie bezpieczeństwa informacji. Wszyscy pracownicy muszą być świadomi swoich obowiązków w zakresie ochrony danych.
 - h. Zarządzanie dostępem – norma wymaga, aby dostęp do informacji i zasobów organizacji był kontrolowany i ograniczony na podstawie ról i odpowiedzialności pracowników.
 - i. Monitorowanie i przeglądy – norma określa, że organizacje muszą regularnie monitorować skuteczność wdrożonego systemu zarządzania bezpieczeństwem informacji oraz przeprowadzać audyty, które pozwolą ocenić zgodność z wymaganiami normy.
 - j. Zgodność z przepisami prawa – norma wymaga, aby organizacje zapewniały zgodność z obowiązującymi przepisami prawnymi dotyczącymi ochrony danych osobowych, ochrony prywatności i bezpieczeństwa informacji.
16. Za równoważną do regulacji RoHS Zamawiający uzna regulację, która dotyczy stosowania substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym w minimum następującym zakresie:
- a. Zakaz stosowania niebezpiecznych substancji – ogranicza użycie sześciu substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym: ołów (Pb), rtęć (Hg), kadm (Cd), sześciowartościowy chrom (Cr⁶), polibromowane bifenyle (PBB) i polibromowane etery difenylowe (PBDE).
 - b. Zastosowanie do sprzętu elektronicznego i elektrycznego – obejmuje szeroki zakres produktów, takich jak telewizory, komputery, sprzęt AGD, zabawki, oświetlenie LED, urządzenia medyczne, sprzęt telekomunikacyjny i inne urządzenia elektroniczne.
 - c. Zobowiązanie producentów do zgodności – Producenci i importerzy sprzętu elektrycznego i elektronicznego muszą zapewnić, że ich produkty nie zawierają zabronionych substancji powyżej dopuszczalnych poziomów.
 - d. Oświadczenia o zgodności – Producenci są zobowiązani do dostarczania odpowiednich oświadczeń o zgodności z regulacją. Powinny one być udostępniane organom nadzoru oraz użytkownikom w razie potrzeby.
 - e. Kontrola i nadzór rynkowy – regulacja nakłada obowiązek przeprowadzania kontroli rynkowych przez odpowiednie organy państwowe, aby upewnić się, że produkty wprowadzane na rynek UE spełniają wymogi dyrektywy.
 - f. Ograniczenie wpływu na zdrowie i środowisko – celem regulacji jest zmniejszenie negatywnego wpływu niebezpiecznych substancji na zdrowie ludzi oraz na środowisko naturalne, szczególnie podczas recyklingu i utylizacji odpadów elektronicznych.
 - g. Zdolność do recyklingu i odzysku – regulacja promuje projektowanie produktów w sposób, który umożliwia ich łatwiejszy recykling i utylizację. Przepisy zakładają, że zabronione substancje nie mogą występować w produktach w ilościach, które utrudniają ich odzyskiwanie.

- h. Zakres geograficzny – regulacja ma zastosowanie w krajach Unii Europejskiej oraz w krajach, które przyjęły odpowiednie przepisy zgodne z dyrektywą.
 - i. Obowiązki w przypadku modyfikacji produktów – W przypadku wprowadzenia istotnych zmian w produkcie (np. zmiana jego konstrukcji), producent musi upewnić się, że nowa wersja również spełnia wymagania regulacji. Dotyczy to również produktów wprowadzanych na rynek wtórny (np. w ramach naprawy lub refabrykacji).
17. Za równoważną do regulacji CE Zamawiający uzna regulację, która spełnia wszystkie odpowiednie wymagania dotyczące zdrowia, bezpieczeństwa oraz ochrony środowiska, zgodnie z przepisami UE w minimum następującym zakresie:
- a. Potwierdzenie zgodności z wymaganiami UE – formalne oświadczenie producenta lub importera, że dany produkt spełnia wszystkie obowiązujące przepisy unijne dotyczące zdrowia, bezpieczeństwa, ochrony środowiska i innych przepisów regulujących dany produkt.
 - b. Oznakowanie CE – posiada system oznaczeń, który wskazuje, że produkt przeszedł ocenę zgodności i jest dopuszczony do sprzedaży w Unii Europejskiej.
 - c. Szczegółowe informacje o producencie – dokument potwierdzający musi zawierać pełne dane producenta (lub importera), takie jak nazwa firmy, adres siedziby, a także dane kontaktowe. W przypadku importera – także informacje o tym, kto odpowiada za dany produkt w UE.
 - d. Opis produktu – dokument potwierdzający musi zawierać szczegółowy opis produktu, który obejmuje nazwę produktu, numer referencyjny lub numer katalogowy, a także inne identyfikatory, które umożliwiają jednoznaczną identyfikację produktu.
 - e. Odniesienia do odpowiednich norm – dokument potwierdzający wskazuje normy, dyrektywy lub przepisy unijne, z którymi produkt jest zgodny.
 - f. Procedura oceny zgodności – dokument potwierdzający musi wskazywać, w jaki sposób ocena zgodności produktu została przeprowadzona (np. przez samodzielną ocenę producenta lub poprzez współpracę z jednostką notyfikowaną w przypadku bardziej skomplikowanych produktów).
 - g. Data i miejsce sporządzenia deklaracji – dokument potwierdzający powinien zawierać datę sporządzenia deklaracji oraz miejsce jej podpisania, co ma znaczenie prawne i daje pewność co do okresu ważności oświadczenia.
 - h. Podpis osoby upoważnionej – dokument potwierdzający musi być podpisana przez osobę upoważnioną w imieniu producenta lub importera, która jest odpowiedzialna za prawdziwość oświadczenia. Zwykle jest to przedstawiciel firmy, który ma uprawnienia do składania oświadczeń w imieniu organizacji.
 - i. Wymóg dostępności dla organów nadzoru – dokument potwierdzający musi być dostępny dla odpowiednich organów nadzoru rynkowego, które mogą przeprowadzać kontrole w celu weryfikacji zgodności produktów z obowiązującymi wymaganiami.
 - j. Zakres odpowiedzialności producenta – dokument potwierdzający musi być dokumentem, który wiąże producenta z odpowiedzialnością za zgodność produktu z wymaganiami prawnymi i normatywnymi. Jeżeli produkt nie spełnia wymagań, producent lub importer mogą być pociągnięci do odpowiedzialności za naruszenie przepisów UE.

18. Za równoważną do certyfikacji FIPS 140-2 Zamawiający uzna certyfikację, która dotyczy standardu wymagań bezpieczeństwa dla modułów kryptograficznych w minimum następującym zakresie:

- a. Obejmuje wszystkie komponenty sprzętowe, oprogramowanie i kombinacje tych elementów, które realizują operacje kryptograficzne (np. szyfrowanie, podpisy cyfrowe, generowanie kluczy).
- b. Wymaga, aby moduły kryptograficzne posiadały odpowiednią ochronę przed manipulacjami fizycznymi.
- c. Wymaga, aby wszystkie klucze kryptograficzne były odpowiednio chronione. Obejmuje to m.in. przechowywanie, generowanie, zarządzanie i wymianę kluczy w sposób, który zapobiega ich nieautoryzowanemu ujawnieniu.
- d. Nakłada wymagania dotyczące bezpiecznego uruchamiania modułu kryptograficznego, w tym procedury inicjalizacji, które muszą zapewniać, że urządzenie jest w pełni zabezpieczone przed uruchomieniem jakichkolwiek operacji kryptograficznych.
- e. Wymaga, aby systemy kryptograficzne były testowane pod kątem zabezpieczeń kryptograficznych.
- f. Definiuje wymagania dotyczące implementacji standardowych algorytmów kryptograficznych.
- g. Wymaga, aby systemy kryptograficzne były odpowiednio utrzymywane przez cały okres ich użytkowania.

3. Przedmiot zamówienia dla części nr 1.

3.1. Wymagania ogólne.

1. Zamówienie będzie realizowane na rzecz Urzędu Miasta Przasnysza oraz następujących jednostek organizacyjnych:
 - 1) Ośrodek Sportu i Rekreacji w Przasnyszu;
 - 2) Szkoła Podstawowa nr 1 z Oddziałami Integracyjnymi im. Kawalerów Orderu Uśmiechu w Przasnyszu;
 - 3) Szkoła Podstawowa nr 2 im. Henryka Sienkiewicza w Przasnyszu;
 - 4) Szkoła Podstawowa nr 3 im. Tadeusza Kościuszki w Przasnyszu;
 - 5) Żłobek Miejski w Przasnyszu;
 - 6) Miejskie Przedszkole Nr 1 im. Marii Kownackiej w Przasnyszu;
 - 7) Miejskie Przedszkole nr 2 z Oddziałami Integracyjnymi w Przasnyszu;
 - 8) Miejski Ośrodek Pomocy Społecznej;
 - 9) Środowiskowy Dom Samopomocy w Przasnyszu.
2. Wykonawca jest zobowiązany do przeprowadzenia w poszczególnych latach realizacji projektu pn. „Cyberbezpieczny Samorząd” współfinansowanego w ramach środków Unii Europejskiej i budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytetu II: Zaawansowane usługi cyfrowe, Działania 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, tj. w latach 2025 i 2026 audytu systemu zarządzania bezpieczeństwem informacji w związku z zapisami w § 19 ust. 2 pkt 14 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. 2024 poz. 773), zwanego dalej „audytem KRI” dla Zamawiającego.
3. Wykonawca jest odpowiedzialny za przeprowadzenie aktualizacji i wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) dla Zamawiającego.
4. Zakres audytu systemu bezpieczeństwa informacji każdorazowo obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI oraz zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023 dla Zamawiającego.
5. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.
6. Audyt KRI oraz aktualizacja i wdrożenie SZBI dla Zamawiającego muszą zostać przeprowadzone przez:
 - 1) 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;
 - 2) 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-EN ISO/IEC 27001:2023.
7. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z częściowo wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego

oraz uwzględnić w ramach aktualizacji i wdrożenia SZBI planowany w ramach realizacji projektu zakres usprawnień SZBI.

8. Wykonawca po wykonaniu ostatniego audytu KRI jest zobowiązany do uzupełnienia ankiety dojrzałości cyberbezpieczeństwa. Ankietę dojrzałości cyberbezpieczeństwa należy wypełnić w oparciu o aktualny na dzień wypełnienia ankiety wzór ankiety opublikowany na stronie: <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad> (załącznik nr 6 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych).
9. Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie na wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta” dla Zamawiającego na podstawie zebranych przez Wykonawcę danych. Zamawiający nie dopuszcza pozostawienia pustych pól dla określonych powyżej kolumn, w przypadku jeżeli w polu opisowym nie przewiduje się zmian wówczas należy zamieścić odpowiednią informację. Ankieta dojrzałości cyberbezpieczeństwa zostanie podpisana przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczona do Zamawiającego w formie elektronicznej.
10. Jednostki samorządu terytorialnego oraz jego jednostki podległe, które biorą udział w projekcie „Cyberbezpieczny Samorząd” są zobowiązane do przesłania do NASK raportu z audytu KRI oraz wypełnionej ankiety dojrzałości cyberbezpieczeństwa. Niezwłocznie po ich przekazaniu przez Wykonawcę dokumenty te zostaną przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z tej dokumentacji przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze także powyżej wskazany cel przeprowadzenia zamówienia i jego przeznaczenie.
11. Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem zarówno w trakcie realizacji zamówienia jak i w trakcie okresu gwarancji.
12. Wykonawca zrealizuje zamówienie w oparciu o dokumentację, którą Zamawiający dysponuje niezależnie od realizacji przedmiotu umowy i o wyjaśnienia udzielane przez Zamawiającego. W szczególności realizacja przedmiotu umowy przez Wykonawcę nie może być uwarunkowana wytwarzaniem lub uzupełnianiem dokumentów i opracowań przez Zamawiającego w związku z realizacją przedmiotu umowy, tj. Zamawiający nie może być zobowiązany do wypełniania ankiet, kwestionariuszy, sporządzania notatek itp., a informacje niezbędne Wykonawcy do wykonania przedmiotu umowy mogą być pozyskiwane wyłącznie w postaci materiałów źródłowych i wywiadu bezpośredniego.

13. Zamawiający dopuszcza prowadzenie prac związanych z: analizą dokumentacji, opracowaniem dokumentacji i polityk, opracowania raportów poza siedzibą Zamawiającego. Zamawiający nie dopuszcza prowadzenia instruktaży, konsultacji, audytów, analiz stanu istniejącego i określenie stanu faktycznego zabezpieczeń technicznych w formule zdalnej, tj. w postaci on-line lub innej poza siedzibą Zamawiającego.
14. Zamawiający nie dopuszcza aby poszczególne etapy realizacji usługi aktualizacji i wdrożenia SZBI wskazane w dalszej części dokumentu realizowane były w dniach następujących po sobie, Zamawiający zakłada co najmniej 7 dni roboczych przerw pomiędzy etapami. Wymóg dotyczy urzędu i jego jednostek organizacyjnych biorących udział w projekcie.
15. Zamawiający wymaga aby każdy etap (lub jego część) realizacji usługi aktualizacji i wdrożenia SZBI wskazany w dalszej części dokumentu był realizowany w siedzibie Urzędu i jego jednostkach organizacyjnych w czasie nie krótszym niż jeden dzień roboczy odrębnie dla Urzędu i jego jednostek organizacyjnych biorących udział w projekcie.
16. Zamawiający wymaga aby każdy audyt był realizowany w siedzibie Urzędu i jego jednostkach organizacyjnych w czasie nie krótszym niż jeden dzień roboczy odrębnie dla Urzędu i jego jednostek organizacyjnych biorących udział w projekcie.
17. Na wszystkie usługi Wykonawca udzieli gwarancji do dnia 30.06.2026 r. polegającej na wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w okresie gwarancji.

3.2. Zakup usług aktualizacji i wdrożenia SZBI.

Celem usługi w ramach działania będzie aktualizacja i wdrożenie procedur systemu zarządzania bezpieczeństwem informacji wdrożonych u Zamawiającego z uwzględnieniem uwarunkowań i specyfiki projektu oraz specyfiki jednostek. W efekcie zostanie zaktualizowana także polityka bezpieczeństwa w zakresie ochrony danych osobowych. Usługa obejmuje również aktualizację dokumentów opisujących zbiory danych i ich zgodność z wymogami prawnymi oraz aktualizację dokumentów opisujących miejsca i sposoby przetwarzania danych osobowych.

Na usługę aktualizacji, opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji składają się co najmniej:

1. Wykonanie oceny obecnej dostępnej dokumentacji.
2. Określenie stanu faktycznego zabezpieczeń danych w systemach informatycznych poprzez przeprowadzenie audytu zabezpieczeń dostępu do danych oraz przygotowanie raportu wraz z zaleceniami i projektem zmian spełnienie wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych.
3. Przeprowadzenie instruktażu wprowadzającego dla pracowników w zakresie ochrony informacji, inwentaryzacji aktywów informacyjnych oraz oceny ryzyka.
4. Aktualizacja/opracowanie Polityki Bezpieczeństwa zgodnej z wymaganiami normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych w zakresie:
 - 1) organizacja systemu bezpieczeństwa informacji;
 - 2) zarządzanie aktywami;

- 3) zarządzanie zasobami ludzkimi;
 - 4) organizacja bezpieczeństwa fizycznego i środowiskowego;
 - 5) zarządzanie komunikacją i eksploatacją;
 - 6) rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania;
 - 7) kontrola dostępu, zarządzania hasłami, stosowania zabezpieczeń kryptograficznych, czystego biurka i czystego ekranu, usuwania i niszczenia informacji, pracy w strefach bezpieczeństwa;
 - 8) akwizycja, rozwój i utrzymanie systemu;
 - 9) zarządzanie incydentami związanymi z bezpieczeństwem informacji;
 - 10) zarządzanie ciągłością działania;
 - 11) zarządzania kopiami zapasowymi;
 - 12) zarządzania monitoringiem;
 - 13) zobowiązanie do zachowania poufności, stosowania polityk i procedur SZBI;
 - 14) używania urządzeń komputerowych;
 - 15) metoda szacowania i postępowania z ryzykiem;
 - 16) deklaracja stosowania
5. Wdrożenie Polityki Bezpieczeństwa Informacji. Poprzez wdrożenie należy rozumieć także aktualizację/utworzenie odpowiednich dokumentów po konsultacjach z pracownikami Zamawiającego, zatwierdzenie dokumentacji przez Kierownictwo Zamawiającego oraz przeprowadzenie instruktażu pracowników w zakresie wykonywania obowiązków zgodnie z opracowanym sposobem postępowania w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Ponad to:

1. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedury bezpieczeństwa fizycznego obejmujące obowiązek wyznaczania osoby odpowiedzialnej za bezpieczeństwo fizyczne.
2. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zasady odpowiedzialności za cyberbezpieczeństwo wraz ze wskazaniem obowiązku wyznaczania osoby odpowiedzialnej za cyberbezpieczeństwo.
3. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń z zakresu cyberbezpieczeństwa wraz z wprowadzeniem obowiązku regularnego, corocznego prowadzenia szkoleń.
4. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje treść zarządzenia wdrażającego SZBI dla Zamawiającego.
5. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzykiem obejmujący systematyczne tworzenie raportów oceny ryzyka w Jednostce oraz konieczność cyklicznego przeglądu tego raportu przez Kierownika JST.
6. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje szczegółowy sposób realizacji celów oraz we współpracy z Zamawiającym przypisze odpowiedzialności za ich realizację.
7. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedurę wprowadzającą obowiązek regularnego, corocznego przeglądu PBI jednostki.
8. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń obejmującą obowiązek informowania o zmianach w PBI w toku okresowych szkoleń stanowiskowych.
9. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kluczowe aktywa informacyjne Jednostki (zbiory danych/systemy/usługi).

10. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje rejestr ryzyk uwzględniający aktywa Jednostki.
11. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zagrożenia związane z cyberbezpieczeństwem w ramach procesów zarządczych oraz zarządzania ryzykiem.
12. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzykiem związanym z zagrożeniami bezpieczeństwa informacji.
13. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek używania do określenia w Jednostce zagrożeń, podatności, prawdopodobieństwa ich wystąpienia i skutków.
14. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek identyfikacji i priorytetyzacji odpowiedzi na ryzyka.
15. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą system oceny ryzyka.
16. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem cyberbezpieczeństwa uwzględniającą identyfikowane, ustanawiane i oceniane ryzyka.
17. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania danymi uwzględniającą polityki ich niszczenia, plan backup, plany reagowania i odtwarzania danych.
18. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami.
19. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania zapisami zdarzeń / logów/ inspekcji.
20. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę użytkowania dostępu do odczytu lub zapisu danych z zewnętrznych nośników danych.
21. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów.
22. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami uwzględniający obowiązek dokumentowania ryzyka z nimi związanego.
23. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów i ich aktualizacji w obszarze doświadczeń i wniosków z wykrytych i obsługiwanych incydentów.
24. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów wraz z obowiązkiem ich aktualizacji.
25. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę planów odtwarzania uwzględniającą obowiązek ich aktualizacji w obszarze doświadczeń i wniosków z prowadzonych procesów odtwarzania.

Poszczególne etapy realizacji usługi.

Etap I. Audyt zerowy.

1. Określenie stanu spełnienia wymagań prawnych nałożonych na organizację w zakresie ochrony informacji.

2. Sprawdzenie spełnienia wymagań i zaleceń w ramach standardów PN-EN ISO/IEC 27001:2023 i norm pokrewnych.
3. Inwentaryzacja aktywów informacyjnych i ocena ryzyka.
4. Ocena zabezpieczeń technicznych, organizacyjnych oraz fizycznych.
5. Analiza dokumentacji Polityki Bezpieczeństwa Informacji.
6. Analiza dokumentacji Polityki Bezpieczeństwa Danych Osobowych.
7. Zestaw działań mających na celu określenie stanu faktycznego zabezpieczeń technicznych w systemie informatycznym:
 - 1) Ocena schematu sieci.
 - 2) Określenie rodzaju połączeń.
 - 3) Określenie segmentów sieci.
 - 4) Przeprowadzenie oceny środowiska informatycznego.
 - 5) Ocena sposobu identyfikowania i logowania użytkowników.
 - 6) Analiza zarządzania kontami użytkowników.
 - 7) Analiza strony www i BIP pod kątem ochrony danych osobowych.
 - 8) Analiza systemu backupów i archiwizacji danych.
 - 9) Określenie miejsc redundancji w sieci i systemach informatycznych.
 - 10) Analiza konfiguracji zabezpieczeń systemów operacyjnych na serwerach.
 - 11) Analiza konfiguracji zabezpieczeń baz danych.
 - 12) Określenie bezpieczeństwa aplikacji i serwerów WWW.
 - 13) Analiza konfiguracji urządzeń sieciowych: switchy, routery, IDS, IPS, UTM, firewall.
 - 14) Ocena zabezpieczeń dostępu do sieci publicznej.
 - 15) Badanie podatności systemów operacyjnych za pomocą specjalistycznego oprogramowania.
 - 16) Analiza zabezpieczeń stacji roboczych.
 - 17) Analiza ochrony danych na komputerach przenośnych.
 - 18) Badanie zabezpieczeń nośników zewnętrznych.
 - 19) Sprawdzenie procedur zarządzania ciągłością działania.
8. Opracowanie raportu z audytu zerowego zawierającego analizę bezpieczeństwa i adekwatności zabezpieczeń stosowanych przez Zamawiającego w odniesieniu do sieci i systemów informatycznych oraz rodzaju danych w nich przetwarzanych, z uwzględnieniem obowiązujących przepisów prawa, zasad wiedzy technicznej, wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych.

Etap II. Zastosowanie zabezpieczeń na podstawie zaleceń poaudytowych.

1. Konsultacje przy wdrożeniu zabezpieczeń w infrastrukturze systemu informatycznego;
2. Konsultacje przy wdrożeniu zabezpieczeń organizacyjnych – polityki bezpieczeństwa danych osobowych, zapisów w umowach z dostawcami itp.

Etap III. Planowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

1. Przeprowadzenie instruktażu dla kadry zarządzającej z zasad bezpieczeństwa informacji.
2. Zakres SZBI:
 - 1) określenie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
 - 2) określenie zasięgu organizacji;

- 3) badanie środowiska zewnętrznego, powiązań z innymi organizacjami, systemami oraz dostawcami.
3. Zdefiniowanie wymaganych polityk SZBI:
 - 1) uwzględnienie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
 - 2) analiza wymagań prawnych oraz wymagań wynikających z umów;
 - 3) uwzględnienie sposobu ustalania celów oraz wyznaczania kierunków działań w ramach systemu.
4. Szacowanie ryzyka:
 - 1) wybór metody szacowania ryzyka;
 - 2) określenie kryteriów akceptowalności ryzyk i identyfikacji akceptowalnych poziomów ryzyk;
 - 3) zdefiniowanie obszarów zabezpieczeń objętych analizą ryzyka.
5. Wybór celów zabezpieczeń:
 - 1) zdefiniowanie celów zabezpieczeń na podstawie listy zawartej w załączniku A normy PN-EN ISO/IEC 27001:2023;
 - 2) zdefiniowanie własnych celów zabezpieczania i zabezpieczeń;
 - 3) uwzględnienie wyników procesu szacowania ryzyka i określenie postępowania z ryzykiem;
 - 4) określenie środków ochrony.

Etap IV. Inwentaryzacja i szacowanie ryzyka SZBI.

1. Przeprowadzenie instruktaży dla pracowników oraz kadry zarządzającej z metody inwentaryzacji i klasyfikacji aktywów informacyjnych.
2. Wykonanie wraz z pracownikami inwentaryzacji i klasyfikacji aktywów informacyjnych.
3. Zdefiniowanie planu postępowania z ryzykiem:
 - 1) przeprowadzenie instruktaży dla kadry zarządzającej z wybranej metody oceny ryzyka;
 - 2) szacowanie i ocena ryzyka – zaktualizowanie wartości ryzyka wynikające z audytu zerowego;
 - 3) zdefiniowanie planu postępowania z ryzykiem;
 - 4) określenie planu zarządzania zidentyfikowanymi i oszacowanymi ryzykami;
 - 5) określenie zadań do realizacji, zdefiniowanie odpowiedzialności i ram czasowych.
4. Opracowanie raportu z oceny ryzyka.

Etap V. Opracowanie niezbędnej dokumentacji SZBI.

1. Opracowanie wspólnie z pracownikami Zamawiającego wymaganych procedur i instrukcji:
 - 1) opracowanie Polityki Bezpieczeństwa Informacji;
 - 2) opracowanie Instrukcji Zarządzania Systemem Informatycznym;
 - 3) opracowanie procedur i instrukcji wymaganych przez normę PN-EN ISO/IEC 27001:2023;
 - 4) opracowanie procedur i instrukcji dopasowanych do specyfiki działalności organizacji;
 - 5) opracowanie Instrukcji postępowania na wypadek wykrycia incydentu naruszenia bezpieczeństwa;
 - 6) opracowanie procedury audytu wewnętrznego;
 - 7) opracowanie procedury nadzoru nad dokumentacją;
 - 8) opracowanie procedury działań korygujących i zapobiegawczych;
 - 9) opracowanie procedury zachowania ciągłości działania;
 - 10) opracowanie wraz z pracownikami Zamawiającego planów ciągłości działania.

2. Wykonanie projektu zabezpieczeń - opracowanie projektu zabezpieczeń i konsultacje przy wdrożeniu odpowiednio skutecznych zabezpieczeń zgodnych z celami zabezpieczeń.
3. Opracowanie programu uświadamiania i szkolenia.
4. Przeprowadzenie instruktaży dla pracowników z dokumentacji ochrony informacji.
5. Przeprowadzenie instruktaży dla kadry zarządzającej z dokumentacji ochrony informacji.

Etap VI. Weryfikacja i monitorowanie SZBI.

1. Przeprowadzenie wraz z pracownikami organizacji audytu wewnętrznego.
2. Opracowanie raportu z audytu wewnętrznego.
3. Przeprowadzenie wraz z pracownikami organizacji przeglądu systemu SZBI:
 - 1) przegląd zagrożeń;
 - 2) przegląd podatności;
 - 3) określenie i weryfikacja ryzyk;
 - 4) weryfikacja planu postępowania z ryzykiem;
 - 5) sprawdzenie zabezpieczeń i celów zabezpieczeń;
 - 6) określenie zgodności zakresu SZBI;
 - 7) weryfikacja zgodności z politykami i celami zabezpieczeń;
 - 8) przegląd i ocena skuteczności zabezpieczeń;
 - 9) weryfikacja zgodności wykorzystywania procedur;
 - 10) weryfikacja zgodności obowiązków i uprawnień w ramach SZBI;
 - 11) analiza audytów bezpieczeństwa;
 - 12) weryfikacja dokumentacji i sposobu postępowania z incydentami;
 - 13) weryfikacja sugestii oraz informacji zwrotnych od zainteresowanych stron;
 - 14) sprawdzenie aktualności procedur ciągłości działania.
4. Opracowanie raportu z przeglądu.

3.3. Zakup usług przeprowadzenia audytu zgodności KRI.

Zakres audytu systemu bezpieczeństwa informacji (zwany na potrzeby przedmiotowego postępowania audytem zgodności KRI, audytem KRI) obejmie zgodność z kryteriami zawartymi w Rozporządzeniu KRI oraz zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023 dla Zamawiającego i dotyczyć będzie istniejącej na czas przeprowadzenia audytu dokumentacji systemu zarządzania bezpieczeństwem oraz warunków technicznych bezpieczeństwa informacji (BI) zgodnie z minimalnymi wymaganiami wykonania usługi określonymi poniżej.

Wymagania minimalne wykonania usługi:

1. Przedmiotem zamówienia jest przeprowadzenie audytu dotyczącego spełnienia wymagań normy PN-EN ISO/IEC 27001:2023 oraz 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. 2024 poz. 773), zwanym dalej „Rozporządzeniem KRI”.
2. Audyt KRI 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.

3. Określenie minimalnego zakresu audytowanych obszarów:
- a) świadczenie usług w formie elektronicznej w tym udostępnionej na platformie ePUAP, zgodnie z art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2024 poz. 307);
 - b) zamieszczenie na głównej stronie internetowej podmiotu (i/lub na stronie BIP), odesłania do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw, zgodnie z § 5 ust. 2 pkt 1 i 4 Rozporządzenia KRI;
 - c) poziom wspierania modelu usługowego w procesie świadczenia usług elektronicznych przez systemy teleinformatyczne podmiotu, zgodnie z §15 ust. 2 Rozporządzenia KRI;
 - d) poziom współpracy systemów teleinformatycznych z innymi systemami podmiotu publicznego lub systemami informatycznymi innych podmiotów publicznych w tym rejestrach referencyjnymi, zgodnie z §5 ust. 3 pkt 3 Rozporządzenia KRI;
 - e) sposób komunikacji z innymi systemami w tym wyposażenie w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących zapewniających BI, zgodnie z §16 ust. 1 Rozporządzenia KRI;
 - f) regulacje wewnętrzne opisujące sposób zarządzania dokumentacją, w tym zakres stosowania elektronicznego obiegu dokumentów, zgodnie z §19 ust. 2 pkt 9 Rozporządzenia KRI;
 - g) sposób kodowania znaków w dokumentach wysyłanych i odbieranych z systemów teleinformatycznych podmiotu, zgodnie z §17 ust. 1 Rozporządzenia KRI;
 - h) sposób udostępniania zasobów informatycznych z systemów teleinformatycznych, zgodnie z §18 ust. 1 Rozporządzenia KRI;
 - i) sposób przyjmowania dokumentów elektronicznych przez systemy teleinformatyczne, zgodnie z §18 ust. 2 Rozporządzenia KRI;
 - j) dokumentacja SZBI, w tym Polityka BI oraz inne dokumenty stanowiące SZBI, Dokumentacja przeglądów SZBI, szacowania ryzyka, audytów, incydentów naruszenia BI, zgodnie z §19 ust. 1 Rozporządzenia KRI;
 - k) działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia będące konsekwencją wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI, zgodnie z §19 ust. 2 pkt 1 Rozporządzenia KRI;
 - l) stopień zaangażowania kierownictwa podmiotu w proces ustanawiania i funkcjonowania SZBI oraz zarządzania BI (przeglądy SZBI, szacowanie i obsługa ryzyka BI, egzekwowanie działań związanych z BI), zgodnie z §19 ust. 2 Rozporządzenia KRI;
 - m) regulacje wewnętrzne opisujące sposób zarządzania ryzykiem BI w podmiocie;
 - n) dokumentacja z przeprowadzania okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestr ryzyk, zawierający informacje o zidentyfikowanych ryzykach, ich poziomie, plan postępowania z ryzykiem, zgodnie z §19 ust. 2 pkt 3 Rozporządzenia KRI;
 - o) działania minimalizujące ryzyko zgodnie z planem postępowania z ryzykiem stosownie do szacowania ryzyka;

- p) regulacje wewnętrzne opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych;
- q) rejestr zasobów teleinformatycznych zawierający informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkownika, zgodnie z §19 ust. 2 pkt 2 Rozporządzenia KRI;
- r) sposób aktualizacji rejestru zasobów teleinformatycznych;
- s) regulacje wewnętrzne opisujące zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym do przetwarzania danych osobowych;
- t) adekwatność poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji, w tym upoważnień do przetwarzania danych osobowych (rejestr wydanych upoważnień), zgodnie z §19 ust. 2 pkt 4 Rozporządzenia KRI;
- u) działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych, w tym przeglądy w celu wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie itp.;
- v) sposób i szybkość odbierania uprawnień byłym pracownikom w systemach informatycznych, zgodnie z §19 ust. 2 pkt 5 Rozporządzenia KRI;
- w) regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych w procesie przetwarzania informacji w systemach teleinformatycznych;
- x) dokumentacja z przeprowadzonych szkoleń pod kątem zakresu tematycznego, w tym: aktualności informacji o zagrożeniach, skutkach i zabezpieczeniach, wskaźnik liczby osób przeszkolonych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, a także cykliczności szkoleń, zgodnie z §19 ust. 2 pkt 6 Rozporządzenia KRI;
- y) regulacje wewnętrzne określające zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, zgodnie z §19 ust. 2 pkt 8 Rozporządzenia KRI;
- z) działania w zakresie stosowania zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, w tym stosowania zabezpieczeń i procedur bezpieczeństwa przez użytkowników urządzeń przenośnych i pracy na odległość;
- aa) umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych w zakresie zapisów gwarantujących odpowiedni poziom BI, zgodnie z §19 ust. 2 pkt 1 Rozporządzenia KRI;
- bb) regulacje wewnętrzne, w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji;
- cc) sposób zgłaszania i postępowania z incydentami (działania korygujące), rejestr incydentów naruszenia BI, wpływ analizy incydentów na SZBI, ewentualna współpraca z CERT.GOV.PL, zgodnie z §19 ust. 2 pkt 13 Rozporządzenia KRI;
- dd) regulacje wewnętrzne, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie BI;
- ee) sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z §19 ust. 2 pkt 14 Rozporządzenia KRI;
- ff) działania podjęte w wyniku zaleceń poaudytowych;

- gg) określenie zasad tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów podmiotu, zgodnie §19 ust. 2 pkt 12 lit. b rozporządzenia KRI;
 - hh) działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów oraz dokumentacja z tych działań;
 - ii) regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych, w tym plan postępowania z ryzykiem, zgodnie z §19 ust. 2 pkt 11 Rozporządzenia KRI;
 - jj) regulacje wewnętrzne dotyczące zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie, zgodnie z §19 ust. 2 pkt 7 i 9 Rozporządzenia KRI;
 - kk) działania związane z monitorowaniem dostępu do informacji np. w systemie informatycznym odnotowującym w bazie danych wszystkie działania użytkowników i administratorów dotyczące systemów teleinformatycznych podmiotu publicznego. Działania związane z monitorowaniem ruchu osobowego w podmiocie, zgodnie z § 19 ust. 2 pkt 7 lit. a) Rozporządzenia KRI;
 - ll) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń serwisowych, analizę rejestru incydentów naruszenia BI, zgodnie z §19 ust. 2 pkt 7 lit. b) Rozporządzenia KRI;
 - mm) działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie zabezpieczeń kryptograficznych, stosowanie systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem, zgodnie z § 19 ust. 2 pkt 7 lit. c) Rozporządzenia KRI;
 - nn) działania związane z ochroną fizyczną informacji zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych, zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem;
 - oo) działania związane z użyciem sprzętu informatycznego i nośników danych a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie BI;
 - pp) regulacje wewnętrzne, w których ustalono zasady w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez opisy stosowania zabezpieczeń, w tym plan postępowania z ryzykiem, zgodnie z §19 ust. 2 pkt 12 oraz ust. 4 Rozporządzenia KRI;
 - qq) regulacje wewnętrzne zawierające zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych, zgodnie z §20 Rozporządzenia KRI;
 - rr) sposób prezentacji informacji na stronach internetowych systemów telekomunikacyjnych podmiotu oraz zgodność z wymogami WCAG2.1.
4. Na podstawie przeprowadzonej analizy dokumentacji oraz audytu bezpieczeństwa, Wykonawca jest zobowiązany przedstawić pisemny raport zawierający wszystkie wyniki, wnioski wraz

z propozycją zmian w zakresie spełnienia wymagań Rozporządzenia KRI. W raporcie muszą zostać uwzględnione wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzelementowej skali: 1) spełnione – oznacza, że wymaganie normy zostało całkowicie wdrożone, 2) częściowo spełnione – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego” jest nieskuteczne wdrożenie procedury (nie przestrzeganie zapisów procedury przez pracowników), 3) niespełnione – wymaganie niespełnione oznacza, że nie zostało ono w ogóle zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.

3.4. Zakup usług szkolenia pracowników z cyberbezpieczeństwa (100 osób).

Wymagania ogólne dla szkoleń:

1. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
2. Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
3. Szkolenia będą odbywać się w dni robocze w godzinach 7.30 – 15.30.
4. Szkolenia będą prowadzone w języku polskim w formule stacjonarnej w siedzibie Zamawiającego. Zamawiający dopuszcza prowadzenie szkoleń w trybie zdalnym w formule on-line.
5. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.
6. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
7. W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda. Dodatkowo, w przypadku szkoleń trwających 8 godzin zaplanowana jest przerwa trwająca 30 minut.
8. W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach. Wykonawca jest zobowiązany do przeprowadzenia szkolenia uzupełniającego dla osób, które nie ze względów przypadków losowych nie będą mogły uczestniczyć w szkoleniu w wyznaczonych terminach.
9. W ramach organizacji szkoleń Wykonawca zapewni:
 - a. Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej lub elektronicznej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto w przypadku organizacji szkoleń w formule stacjonarnej (w siedzibie Zamawiającego), uczestnicy otrzymają materiały pisarskie, w tym zeszyty, długopisy, ołówki itp. Materiały szkoleniowe przekazywane są nieodpłatnie uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.

- b. W przypadku szkoleń prowadzonych w trybie zdalnym w formule on-line Wykonawca jest zobowiązany dostarczyć narzędzia do komunikacji zdalnej, które umożliwią dwustronne przesyłanie przez sieć Internet obrazu i dźwięku między prowadzącym szkolenie a uczestnikami szkolenia. Narzędzie musi umożliwiać zadawanie pytań także w formie pisemnej bezpośrednio na czacie w trakcie trwania sesji szkoleniowej. W przypadku szkolenia prowadzonego w trybie zdalnym w formule on-line Zamawiający zastrzega możliwość nagrania szkolenia, a Wykonawca musi zapewnić wyrażenie na to zgody osoby prowadzącej szkolenie.
- c. W przypadku szkoleń stacjonarnych (w siedzibie Zamawiającego) oraz o ile wynika to z programu szkolenia Wykonawca zapewni sprzęt komputerowy dla każdego uczestnika szkolenia umożliwiający przeprowadzenie szkolenia oraz wystarczającą liczbę własnych licencji na oprogramowanie komputerowe wykorzystywane przy realizacji szkoleń.
- d. Projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń w przypadku prowadzenia szkoleń stacjonarnych (w siedzibie Zamawiającego).
- e. Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym właściwe oznakowanie sal szkoleniowych, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich.
- f. Wydanie uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
- g. Kadre trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
- h. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
 - Lista obecności uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).
 - Lista odbioru zaświadczeń o ukończeniu szkolenia.
 - Potwierdzenie przez uczestników odbioru materiałów szkoleniowych.
 - Przeprowadzenie ankiet satysfakcji po każdym szkoleniu.
 - Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

W ramach ramowego programu szkoleń Zamawiający zaleca ująć następujące zagadnienia:

1. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
2. Polityka bezpieczeństwa w organizacji.
3. Definicja incydentu bezpieczeństwa i zasady postępowania z incydemem.
4. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
5. Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko”.
6. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
7. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.

8. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
9. Prawidłowe korzystanie z oprogramowania antywirusowego.
10. Zasady aktualizacji programów i aplikacji.
11. Szyfrowanie dokumentów i poczty elektronicznej.
12. Polityka haseł, zarządzanie dostępem i tożsamością.

Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolone 100 osób w 12 grupach maksimum 10-osobowych.
2. Szkolenie powinno trwać minimum 6 godzin szkoleniowych dla 1 grupy szkoleniowej.

4. Przedmiot zamówienia dla części nr 2.

4.1. Wymagania ogólne.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów. Niedopuszczalna jest realizacja tylko części funkcji bądź wymaganych standardów zamiast innych określonych jako minimalne w niniejszym dokumencie. Wszystkie wymagania minimalne muszą zostać zapewnione przez dostarczane produkty bez konieczności zakupu żadnych dodatkowych elementów przez Zamawiającego, chyba że z niniejszego dokumentu wynika inaczej.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent

oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

12. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
13. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

4.2. Zakup serwera (1 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji min. 16 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowany jeden procesor maksymalnie szesnastordzeniowy klasy x86 dedykowany do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 235 punktów w teście SPECrate2017_int_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie www.spec.org. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 256 GB, płyta główna musi obsługiwać do min. 1 TB pamięci RAM, co najmniej 10 wolnych slotów na pamięć.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC i/lub Demand Scrubbing i/lub Patrol Scrubbing i/lub Permanent Fault Detection (PFD).
6. Gniazda PCIe: co najmniej dwa wolne sloty w celu możliwości rozbudowy serwera.

7. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024.
8. Interfejsy sieciowe: co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, co najmniej 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT oraz co minimum 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28. Do interfejsów SFP28 dołączone dwie wkładki - moduł optyczny jednomodowy SFP28 LR, prędkość 10/25 Gb, złącze LC duplex.
9. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane min. 14 dysków twardych Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 960 GB każdy oraz zainstalowane min. 2 dyski twarde Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 480 GB każdy. Dodatkowo zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB Hot-Plug w konfiguracji RAID 1. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
10. Kontroler RAID: Sprzętowy kontroler dyskowy, umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
11. Wsparcie dla dysków samoszyfrujących.
12. Wbudowane porty: min. 1 zewnętrzny port VGA, min. 3 zewnętrzne porty USB, w tym co najmniej 1 port USB 3.x, co najmniej 1 port USB musi być dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
13. Wentylatory: Redundantne typu Hot Plug.
14. Zasilacze: Redundantne typu Hot Plug o mocy minimalnej 1100 W każdy.
15. Karta/moduł zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane złącze umożliwiająca zdalne zarządzanie:
 - 1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
 - 2) zdalne monitorowanie i informowanie o statusie serwera,
 - 3) szyfrowane połączenie oraz autentykację i autoryzację użytkownika,
 - 4) możliwość podmontowania zdalnych wirtualnych napędów,
 - 5) wirtualną konsolę z dostępem do myszy, klawiatury,
 - 6) wsparcie dla IPv6,
 - 7) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
 - 8) integracja z Active Directory,
 - 9) wsparcie dla dynamic DNS.
16. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
 - 1) wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
 - 2) blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
 - 3) moduł TPM 2.0;
17. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzanie serwerem klasy Microsoft Windows Server Datacenter w najnowszej wersji oferowanej przez producenta na dzień składania ofert wraz z 70 licencjami dostępowymi umożliwiającymi korzystanie przez 70 użytkowników lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.
Warunki równoważności dla dostawy oprogramowania klasy Microsoft Windows Server Datacenter:

- 1) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nieograniczonej liczbie środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
 - 2) Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
 - 3) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64 TB przez każdy wirtualny serwerowy system operacyjny.
 - 4) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
 - 5) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
 - 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 - 7) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 - 8) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 - 9) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
 - 10) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
 - 11) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 - 12) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
 - 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 - 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
 - 15) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
 - 16) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
 - 17) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
 - 18) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
 - 19) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
 - 20) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
 - 21) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
 - 22) O ile to konieczne ze względu na licencjonowanie producenta oferowanego serwerowego systemu operacyjnego Zamawiający wymaga dostarczenia licencji dostępowych dla 70 użytkowników.
18. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla Microsoft Windows Server 2022, Microsoft Windows Server 2025.

19. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub Certyfikat ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów wymagań w zakresie określonym powyżej.
20. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera.

4.3. Zakup NAS TYP A (2 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa typu RACK z kompletem szyn umożliwiających montaż w szafie.
2. Procesor wielordzeniowy, 64-bitowy x86, ze sprzętowym mechanizmem szyfrowania AES 256bit. Procesor ma osiągać wydajność w testach Cinebench R15 XCPU co najmniej 2100.
3. Pamięć RAM: min. 64 GB.
4. Redundantne zasilanie.
5. Oprogramowanie systemu operacyjnego umożliwiające minimum: zarządzanie i administrację urządzeniem, tworzenie kopii zapasowych z komputerów i serwerów, udostępnianie plików, zarządzanie przestrzenią dyskową, grupowanie dysków, zarządzanie dostępem i użytkownikami, wyszukiwanie plików, kompresowanie plików.
6. Możliwość zainstalowania łącznie 12 dysków 3,5-calowych.
7. Zainstalowane dyski: min. 12 x 2 TB SATA o prędkości min. 6 Gb/s, dyski muszą być zgodne z urządzeniem NAS, tj. które znajdują się na liście zgodności prowadzonej przez producenta urządzenia NAS lub które zostały przetestowane pod kątem zgodności z produktami producenta urządzenia NAS. Wykonawca jest zobowiązany dostarczyć dodatkowo po dwa dyski, o identycznych parametrach jak oferowane, do każdego urządzenia NAS jako dyski zastępcze umożliwiające Zamawiającemu natychmiastową wymianę w przypadku uszkodzenia dysków pracujących w urządzeniu NAS.
8. Wymagane poziomy RAID: RAID 0, 1, 5, 6, 10.

9. Interfejsy sieciowe: min. 2 x Port Gigabit sieci Ethernet (RJ-45); min. 2 x Port 10GbE (RJ-45), min. 2 x Port 10GbE SFP+.
10. Dodatkowo dołączone dwa moduły optyczne jednomodowe SFP+ LR, prędkość 10 Gb/s, złącze LC duplex.
11. Porty USB: min. 2 x USB3.x.
12. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany NAS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta NAS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany NAS wymagań w zakresie określonym powyżej.
13. Co najmniej 60 miesięcy gwarancji producenta.

4.4. Zakup NAS TYP B (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa wolnostojąca.
2. Procesor wielordzeniowy, 64-bitowy x86, ze sprzętowym mechanizmem szyfrowania AES-NI.
3. Pamięć RAM: min. 8 GB.
4. Oprogramowanie systemu operacyjnego umożliwiające minimum: zarządzanie i administrację urządzeniem, tworzenie kopii zapasowych z komputerów i serwerów, udostępnianie plików, zarządzanie przestrzenią dyskową, grupowanie dysków, zarządzanie dostępem i użytkownikami, wyszukiwanie plików, kompresowanie plików.
5. Możliwość zainstalowania łącznie 4 dysków 3,5-calowych.
6. Możliwość zainstalowania do dwóch dysków SSD w celu buforowania lub tworzenia dodatkowych pul pamięci.
7. Zainstalowane dyski: min. 4 x 4 TB, dyski muszą być zgodne z urządzeniem NAS, tj. które znajdują się na liście zgodności prowadzonej przez producenta urządzenia NAS lub które zostały przetestowane pod kątem zgodności z produktami producenta urządzenia NAS. Wykonawca jest zobowiązany dostarczyć dodatkowo dwa dyski o identycznych parametrach jak oferowane do urządzenia NAS jako dyski zastępcze umożliwiające Zamawiającemu natychmiastową wymianę w przypadku uszkodzenia dysków pracujących w urządzeniu NAS.
8. Możliwość opcjonalnej instalacji dysku M.2
9. Wymagane poziomy RAID: 0, 1, 5, 6, 10.
10. Interfejsy sieciowe: 2 x Port 2,5 GbE (RJ-45) z obsługą funkcji Link Aggregation.
11. Porty USB: min. 2 x USB3.2.
12. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany NAS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub

oświadczenia producenta NAS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany NAS wymagań w zakresie określonym powyżej.

13. Co najmniej 60 miesięcy gwarancji producenta.

4.5. Zakup przełączników sieciowych TYP A (4 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzalny przełącznik L3.
2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).
3. Przepustowość routowania/przełączania: min. 200 Gbit/s.
4. Prędkość przekazywania: min. 150 Mpps.
5. Bufor pamięci dla pakietów: max. 3 MB.
6. Rozmiar tablicy MAC: min. 32 000 wpisów.
7. Dostępne interfejsy: min. 48 x 1000Base-T- RJ-45, min. 4 x 10GbE SFP+. Nie są dopuszczane porty SFP+ współdzielone z portami RJ45 (tzw. „combo”). Porty SFP/SFP+ muszą obsługiwać moduły o prędkości transmisji zarówno 1 Gbps jak i 10 Gbps. Dołączone 2 moduły optyczne jednomodowe SFP+ LR, prędkość 10 Gb/s, złącze LC duplex (do każdego urządzenia).
8. Obsługiwane standardy komunikacyjne: 802.3i; 802.3u; 802.3z; 802.3ab; 802.3ae; 802.3ad; 802.3ah; 802.3az; 802.3x; 802.1ab; 802.1w; 802.1s; 802.1p; 802.1q.
9. Obsługiwane protokoły zarządzające: SNMPv1, SNMPv2, SNMPv3, OSPFv2, OSPFv3, RMON.
10. Obsługiwane protokoły sieciowe: IPv4, IPv6, LLDP, MSTP, RSTP, Telnet, TACACS, MLD, RIPv1, RIPv2, OSPFv2, OSPFv3, SSH.
11. Inne cechy: zarządzanie przez www, generowanie raportów zdarzeń systemowych, obsługa min. 4000 sieci VLAN, obsługa multicast, funkcję agregacji portów z wykorzystaniem protokołu LACP, uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia; obsługa list kontroli dostępu (ACL).
12. Możliwość łączenia urządzeń w stos min. 4.
13. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik sieciowy spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta przełącznika sieciowego lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik wymagań w zakresie określonym powyżej.
14. Co najmniej 60 miesięcy gwarancji producenta.

4.6. Zakup przełączników sieciowych TYP B (3 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzany przełącznik L2/L3
2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).
3. Przepustowość routowania/przełączania: min. 35 Gbps.
4. Prędkość przekazywania: min. 20 Mpps.
5. Rozmiar tablicy MAC: min. 8 000 wpisów.
6. Dostępne interfejsy: min. 16 x RJ45 10/100/1000 Mbps; 2 x sloty SFP.
7. Obsługiwane standardy komunikacyjne: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1ad, IEEE 802.1af, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3u.
8. Dodatkowo obsługa: QoS, VLAN, ACL, DHCP, SNMP, Http/Https, SSL, SSH.
9. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik sieciowy spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta przełącznika sieciowego lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik wymagań w zakresie określonym powyżej.
10. Co najmniej 24 miesiące gwarancji producenta.

4.7. Zakup przełączników sieciowych TYP C (12 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzany przełącznik L2/L3
2. Rodzaj obudowy: desktop.
3. Przepustowość routowania/przełączania: min. 14 Gbps.
4. Prędkość przekazywania: min. 20 Mpps.
5. Rozmiar tablicy MAC: min. 8 000 wpisów.
6. Dostępne interfejsy: min. 8 x RJ45 10/100/1000 Mbps.
7. Obsługiwane standardy komunikacyjne: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1ad, IEEE 802.1af, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3u.
8. Dodatkowo obsługa: QoS, VLAN, ACL, DHCP, SNMP, Http/Https, SSL, SSH.
9. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik sieciowy spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta przełącznika sieciowego lub innego dokumentu

potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik wymagań w zakresie określonym powyżej.

10. Co najmniej 24 miesiące gwarancji producenta.

4.8. Zakup UPS TYP A (2 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: RACK, max. 2U, Wykonawca jest zobowiązany dostarczyć szyny do montażu UPS w szafie RACK.
2. Moc pozorna: min. 3 kVA.
3. Architektura UPSa: line-interactive lub online.
4. Liczba i rodzaj gniazdek z utrzymaniem zasilania: 8x IEC C13.
5. Czas podtrzymania dla obciążenia 100%: min. 3 min.
6. Czas podtrzymania przy obciążeniu 50%: min. 12 min.
7. Zabezpieczenia: przeciwprzepięciowe, przeciwzwarceniowe, przeciwprzeciążeniowe.
8. Wyświetlacz LCD lub diody LED sygnalizujące stan pracy urządzenia.
9. Alarmy dźwiękowe urządzenia sygnalizujące stan pracy urządzenia w zakresie określonych przez producenta zdarzeń.
10. Interfejsy: min. 1 x USB, 1 x EPO, 1 x RS-232.
11. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany UPS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta UPS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany UPS wymagań w zakresie określonym powyżej.
12. Co najmniej 36 miesięcy gwarancji producenta.

4.9. Zakup UPS TYP B (54 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: wolnostojąca.
2. Rozmiar obudowy: suma wymiarów obudowy (szerokość + wysokość + głębokość), nie większa niż 65 cm łącznie.
3. Moc wyjściowa: min. 500 W.
4. Napięcie wejściowe: 230 V.
5. Czas przełączania: max. 10 ms.
6. Architektura UPS: line interactive lub online.
7. Ilość gniazd sieciowych: min. 4 typu Schuko.

8. Porty: min. 1 x USB, min. 1x Ethernet.
9. Alarmy i informacje dźwiękowe i wizualne w zależności od rodzaju zdarzenia.
10. Zabezpieczenia: wbudowany moduł regulacji napięcia AVR, zabezpieczenie przeciwprzepięciowe.
11. Czas podtrzymania przy obciążeniu 80 % - min. 1 min.
12. Czas podtrzymania przy obciążeniu 50 % - min. 6 min.
13. Przewód zasilający nie krótszy niż 1 metr.
14. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany UPS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta UPS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany UPS wymagań w zakresie określonym powyżej.
15. Co najmniej 24 miesiące gwarancji producenta.

4.10. Zakup usług backup w chmurze (1 szt.).

Do urządzenia NAS w celu backup danych w zewnętrznej chmurze danych Wykonawca jest zobowiązany zapewnić Zamawiającemu zewnętrzną chmurę danych spełniającą poniżej określone warunki minimalne jej funkcjonowania:

1. Data obowiązywania licencji: 30 czerwiec 2026 r.
2. Ilość danych w chmurze: min. 5 TB.
3. Brak kosztów transmisji danych.
4. Szyfrowanie połączenia przesyłu i transferu danych.
5. Kompatybilność z systemem operacyjnym i oprogramowaniem do tworzenia backupu oferowanego urządzenia NAS.
6. Dostępność danych na poziomie 99 % w danym roku.
7. Do plików i folderów w usłudze chmury można uzyskać dostęp i nimi zarządzać poprzez witrynę lub z poziomu urządzenia NAS.
8. Miejsce składowania danych na obszarze UE.