**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Wykonanie audytów w Starostwie Powiatowym i jednostkach organizacyjnych w ramach projektu „Cyberbezpieczny Powiat Wadowicki” współfinansowanego z **Konkursu Grantowego „Cyberbezpieczny Samorząd”, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.”**

**Podstawy prawne**

* **Dyrektywa 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),**
* Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW
* Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016
* Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2018 r. poz. 1560, z 2019 r. poz. 2020).

**Podstawy merytoryczne**

**PN ISO/IEC 27001:2023** Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji – Wymagania

**ISO/IEC 27701:2019** Techniki bezpieczeństwa - rozszerzenie do ISO / IEC 27001 i ISO / IEC 27002 dla zarządzania informacjami o prywatności - wymagania i wytyczne

**PN ISO/IEC 27002:2022** Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności — Zabezpieczenia informacji

**PN ISO/IEC 27005:2022** Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Wytyczne dotyczące zarządzania ryzykiem związanym z bezpieczeństwem informacji

**PN-EN ISO 22301:2020** Bezpieczeństwo powszechne -- Systemy zarządzania ciągłością działania -- Wymagania.

**Opis i zakres wymagań przedmiotu zamówienia**

**Etap 1: Przeprowadzenie audytu "zerowego" w Starostwie Powiatowym i jednostkach organizacyjnych**

1. **Metodyka audytu:**

Audyty zerowy luki zostanie wykonany na podstawie wybranych wytycznych norm ISO 27001:2023 w kontekście wymagań Dyrektywy NIS2 i Cyber Assessment Framework V3.2 oraz wymagań Konkursu Grantowego „Cyberbezpieczny Samorząd”, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

1. **Zakres prac:**

Przeprowadzenie audytu bezpieczeństwa systemu informacyjnego i ochrony danych u Operatora Usługi Kluczowej będzie odbywać się zgodnie z wymaganiami ustawy z dnia 13 sierpnia 2018 roku o Krajowym Systemie Cyberbezpieczeństwa a także z aktualnymi wymogami prawa, wymaganiami norm PN ISO IEC 27001:2023, PN ISO IEC 22301:2020, Cyber Assessment Framework V3.2, NSC (NIST-800) do oceny cyberdojrzałości i zgodności z wymagań Dyrektywy NIS2, poprzez badanie:

* spełnienia wymogów organizacyjnych obowiązujących u Zamawiającego jako regulacji wewnętrznych normatywnych i operacyjnych dotyczących usługi kluczowej bezpieczeństwa informacji - dokumentacja SZBI/BCM, ochrony danych osobowych – dokumentacja RODO i ODO,
* określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych i testów podatności na reprezentatywnej próbie infrastruktury IT

w celu dokonania oceny stopnia dojrzałości i zgodności organizacyjno-technicznej infrastruktury ICT w kontekście zabezpieczeń konfiguracji, eksploatacji ICT w postaci oceny syntetycznej i graficznej w postaci wykresu.

1. **Opis wymagań: audyt obejmuje tożsame zadania jak dla audytu zerowego luki:**
2. **Audyt organizacyjny polegający na:**
3. weryfikacji środków organizacyjnych (w tym dokumentacja PBI) w obszarze bezpieczeństwa informacji, w tym danych osobowych;
4. weryfikacji procesów i czynności przetwarzania danych uwzględniając ich charakter, zakres, kontekst, cele przetwarzania, zasoby, aktywa i ryzyka
5. weryfikacji realizowania przez pracowników obowiązków wynikających z regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI/BCM/ODO).

Wykaz obowiązków pracowników podlegających weryfikacji (poszczególnych procedur, instrukcji, zapisów z dokumentacji SZBI) zostanie przedłożony Wykonawcy po podpisaniu umowy. Weryfikacja musi obejmować przynajmniej kierownika lub zastępcę kierownika każdej komórki organizacyjnej oraz jej pracowników (chyba, że komórka posiada mniejszą liczbę pracowników - wówczas wszystkich jej pracowników).

1. **Audyt bezpieczeństwa fizycznego**

Badanie polega na weryfikacji środków technicznych służących zabezpieczeniu informacji, w tym danych osobowych, w szczególności stanu bezpieczeństwa fizycznego i środowiskowego siedziby Zamawiającego - budynki i pomieszczenia na podstawie wizji lokalnej obszarów przetwarzania danych.

1. **Audyt teleinformatyczny**

Badanie polega na wykonaniu czynności audytowych na wybranej reprezentatywnej próbie i przeprowadzeniu nieinwazyjnych (wewnętrznych i zewnętrznych) testów penetracyjnych systemów informatycznych, w szczególności odniesieniu do infrastruktury sieciowej, systemu Firewall, aplikacji, portali i wybranych serwisów www oraz poczty elektronicznej, elementów OT jako w trybie hybrydowym:

1. weryfikacji bezpieczeństwa infrastruktury sieciowej, w szczególności:
2. inwentaryzacji urządzeń sieciowych (adresy IP, konfiguracja urządzeń, konfiguracja zapory ogniowej, podział na sieci logiczne i fizyczne) w siedzibie Zamawiającego;
3. analizy urządzeń i ich parametrów technicznych zapewniających stronie Zamawiającej dostęp do sieci Internet - w tym serwera brzegowego, urządzeń UTM, Firewall, routerów;
4. analizy konfiguracji sieci lokalnej;
5. analizy oprogramowania wykorzystywanego przez Zamawiającego w zakresie zabezpieczenia informatycznego;
6. analizy sposobu połączenia segmentów pomiędzy sobą;
7. analizy metody komunikacji pomiędzy segmentami sieci;
8. analizy zabezpieczenia ciągłości działania.
9. weryfikacji bezpieczeństwa infrastruktury serwerowej, w szczególności:
10. analizy bezpieczeństwa zainstalowanych usług (czy zainstalowane oprogramowanie jest aktualne, czy zainstalowane oprogramowanie posiada znane luki w bezpieczeństwie, kto ma dostęp do udostępnionych usług);
11. analizy bezpieczeństwa serwerów pod kątem dostępu użytkowników (czy jedynie uprawnieni użytkownicy mają dostęp do usług, czy udostępnione usługi zawierają jedynie te dane które są wymagane);
12. analizy bezpieczeństwa uprawnień poszczególnych użytkowników oraz grup użytkowników;
13. analizy bezpieczeństwa fizycznego infrastruktury serwerowej;
14. analizy zabezpieczenia ciągłości działania.
15. weryfikacji bezpieczeństwa poczty elektronicznej, domeny, stron internetowych Zamawiającego wg wymagań WCAG 2.1.
16. weryfikacji bezpieczeństwa systemów (aplikacji), w których przetwarzane są dane osobowe:
17. analizy podatności komponentów aplikacji, w tym serwerów aplikacyjnych i baz danych - próby uzyskania dostępu do panelu administracyjnego za pomocą kont zwykłych użytkowników m. in. przez wykorzystanie bieżącej sesji, podniesienie uprawnień, próby uzyskania większych uprawnień, próby uzyskania nieautoryzowanego dostępu do danych znajdujących się w systemie;
18. analizy szyfrowania danych dla danych przesyłanych przez sieci publiczne;
19. Wykazu systemów, w których przetwarzane są dane, w tym dane osobowe w weryfikacji bezpieczeństwa stacji roboczych:

* analiza kontroli dostępu do stacji roboczych,
* analiza zainstalowanego oprogramowania znajdującego się na stacjach roboczych,
* analiza bezpieczeństwa stacji roboczych pod kątem zainstalowanych usług, dostępów zdalnych do stacji roboczych, bezpieczeństwa ochrony antywirusowej.

1. analizy zabezpieczenia ciągłości działania.
2. weryfikacji zarządzania kopiami zapasowymi i ciągłością działania w szczególności:
3. analizy poprawności wykonywanych kopii zapasowych;
4. analizy częstotliwości wykonywania kopii zapasowych;
5. analizy bezpieczeństwa wykonywanych kopii zapasowych;
6. analizy testów odzyskiwania kopii zapasowych - odtwarzania danych w środowisku testowym;
7. analizy zbierania, przechowywania i monitorowania logów systemowych.
8. weryfikacji poprawności realizacji w zakresie:
9. zarządzania hasłami użytkowników i hasłami administracyjnymi;
10. instalacji i aktualizacji oprogramowania;
11. ochrony przed szkodliwym oprogramowaniem;
12. zabezpieczania procesu pracy zdalnej;
13. rozwoju systemów informatycznych;
14. zarządzania zmianami w systemach informatycznych;
15. przeglądów, konserwacji i napraw systemu informatycznego;
16. monitorowania bezpieczeństwa systemów informatycznych,
17. zapisywania, monitorowania, zabezpieczania logów systemowych;
18. monitorowania pojemności i wydajności systemów informatycznych;
19. bezpieczeństwa sieci;
20. zapewnienia legalności oprogramowania;
21. usuwania danych i niszczenia nośników;
22. synchronizacji zegarów;
23. gromadzenia logów.

W czasie wykonania i po wykonaniu usługi, infrastruktura Zamawiającego musi pozostać w niezmienionej formie, tj. nie może zostać uszkodzona, jak również nie mogą zostać usunięte, zmienione, nadpisane dane znajdujące się w tej infrastrukturze. Zamawiający dopuszcza wykonanie audytu w formie hybrydowej.

1. **Raport**

Wynikiem przeprowadzonych audytów i testów będzie raport poaudytowy w standardzie ENISA zawierający:

1. przedmiot, cel i zakres audytu,
2. datę rozpoczęcia audytu,
3. opis przyjętej metodyki,
4. raport dla kierownictwa obejmujący syntezę wyników audytu i ocenę poziomu spełnienia wymogów RODO, regulacji wewnętrznych dot. bezpieczeństwa informacji Zamawiającego oraz ocenę bezpieczeństwa systemu informatycznego, w tym podsumowanie zidentyfikowanych słabości/nieprawidłowości, a także główne rekomendacje dotyczące poprawy bezpieczeństwa informacji, danych i systemu informatycznego.
5. dokładny opis zidentyfikowanych nieprawidłowości, w szczególności:

* wskazujący miejsca, w których występują realne bądź potencjalne problemy z bezpieczeństwem informacji;
* zawierający wyniki audytów, w tym testów i ich interpretację - ustalenia muszą odnosić się do konkretnych przypadków słabości/nieprawidłowości popartych zgromadzonymi dowodami audytowymi, które będą stanowiły załącznik do raportu;
* zawierający rekomendacje w zakresie eliminacji zidentyfikowanych słabości/nieprawidłowości oraz poprawy poziomu bezpieczeństwa, w tym wskazanie działań korygujących i/lub doskonalących bez lokowania sprzętu lub oprogramowania.

1. analizę rekomendowanych zmian w treści regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI) Zamawiającego wraz z proponowaną treścią nowych (zmienionych lub dodanych) zapisów;
2. wypełniony Formularz weryfikacji dojrzałości organizacji pod kątem cyberbezpieczeństwa zgodny z wzorem Ministra Klimatu i Środowiska;
3. datę sporządzenia raportu;
4. imiona i nazwiska audytorów realizujących zadanie etapu oraz ich podpisy.

Wykonawca prześle w formie elektronicznej w formacie edytowalnym i pdf raport, zaszyfrowany programem 7 ZIP przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczony co najmniej 11-znakowym hasłem jednorazowym przesłanym przez alternatywny kanał komunikacji.

1. **Informacje wejściowe do szacowania ceny audytu luki łącznie dla wszystkich wskazanych poniżej lokalizacji**
2. Liczba komputerów:

* Stacjonarnych - 293
* Przenośnych - 125

1. Liczba serwerów:

* Fizycznych - 17
* Wirtualnych - 10

1. Liczba serwerów:

* Windows - 19
* Linux - 8

1. Liczba aplikacji bazodanowych – 58
2. Ilość systemów przetwarzających dane i dane osobowe – 48
3. Liczba serwerowni – 6
4. Liczba urządzeń sieciowych (drukarki, routery, switch, voip, itd.) – 234
5. Liczba Access Point – 26
6. Liczba drukarek sieciowych – 142
7. Liczba podsieci – 27
8. Separacja OT/IT – częściowo
9. Ilość pracowników w dziale IT – 2
10. Liczba pracowników zatrudnionych – 633
11. Ilość lokalizacji z podaniem adresów podlegających weryfikacji audytowej:
12. Starostwo Powiatowe w Wadowicach
    * 1. ul. Stefana Batorego 2, 34-100 Wadowice
13. Powiatowe Centrum Pomocy Rodzinie w Wadowicach
    * 1. ul. Stefana Batorego 2A, 34-100 Wadowice
14. Dom Pomocy Społecznej im. św. O. R. Kalinowskiego
    * 1. ul. gen. K. Pułaskiego 5, 34-100 Wadowice
15. Dom Pomocy Społecznej w Wadowicach
    * 1. ul. Parkowa 1, 34-100 Wadowice
16. Dom Pomocy Społecznej im. św. Brata Alberta w Izdebniku
    * 1. ul. Dworska 150, 34-144 Izdebnik
17. Środowiskowy Dom Samopomocy im. św. Matki Teresy z Kalkuty w Wadowicach
    * 1. ul. E. i K. Wojtyłów 16, 34-100 Wadowice
18. Placówka Opiekuńczo-Wychowawcza w „PROMYK” w Radoczy
    * 1. ul. Dworska 9/2, 34-100 Radocza
19. Placówka Opiekuńczo-Wychowawcza w „Nowy Dom” w Radoczy
    * 1. ul. Dworska 9/2, 34-100 Radocza
20. Ośrodek Interwencji Kryzysowej w Radoczy
    * 1. ul. Dworska 9A, 34-100 Radocza
21. Specjalny Ośrodek Szkolno-Wychowawczy w Kaczynie
    * 1. ul. Krajobrazowa 43, 34-123 Chocznia
22. Specjalny Ośrodek Szkolno-Wychowawczy w Kalwarii Zebrzydowskiej
    * 1. ul. Wł. Niemczynowskiego 1, 34-130 Kalwaria Zebrzydowska
23. Poradnia Psychologiczno-Pedagogiczna w Wadowicach
    * 1. ul. E i K Wojtyłów 16, 34-100 Wadowice
24. Poradnia Psychologiczno-Pedagogiczna w Andrychowie
    * 1. ul. Metalowców 10, 34-120 Andrychów
25. Zespół Szkół Specjalnych w Wadowicach
    * 1. ul. Słowackiego 4, 34-100 Wadowice
26. System SOC – brak

**Etap 2. Przeprowadzenie audytu dokumentacji PBI w Starostwie Powiatowym oraz aktualizacja polityk i procedur**

1. **Przeprowadzenie audytu dokumentacji PBI**

Audyt dokumentacyjny obowiązujących u Zamawiającego Polityk Bezpieczeństwa Informacji oraz procedur związanych z politykami. Wynikiem audytu będzie raport z rekomendacjami w zakresie aktualizacji lub poprawy Polityk Bezpieczeństwa Informacji do zgodności z normatywami ISO 27001, ISO 22301, ISO 20000-1 jako realizacja wymagań Dyrektywy NIS2.

1. **Opracowanie lub aktualizacja dokumentacji obejmująca:**

opracowanie wymagań dokumentacyjnych systemu SZBI /BCM, w zgodnie zapisami Dyrektywy NIS2 z zastosowaniem min. aktualnych norm ISO 27001, ISO 22301, ISO 20000-1 dla wspólnego opisu procesów, przeznaczonej do dalszego wdrożenia dla wskazanych 4 obszarów funkcjonowania Zamawiającego w kontekście wymagań normatywnych aktualnej normy PN-ISO/IEC 27001:2023 dla systemu dokumentacyjnego i obowiązujących normatywne zabezpieczeń, jako wypełnienie obowiązków wynikających z Dyrektywy NIS 2 i Ustawy o Krajowym Systemie Cyberbezpieczeńtwa zgodnie z regulaminem Konkursu Grantowego „Cyberbezpieczny Samorząd”, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.”

tj.

Obszar 1: Zabezpieczenia organizacyjne

Obszar 2: Zabezpieczenia zasobów ludzkich

Obszar 3: Zabezpieczenia fizyczne

Obszar 4: Zabezpieczenia technologiczne

**II.1. Opracowanie dokumentacji systemowej SZBI lub jej aktualizacja:**

1. Określi i sformalizuje zasady zarządzania, w szczególności poprzez wskazanie ról dla osób odpowiedzialnych oraz wskazanie podejścia do zapewnienia zasobów niezbędnych do efektywnego zarządzania bezpieczeństwem i zarządzania usługami.
2. Określi i sformalizuje procedury przeprowadzania audytów bezpieczeństwa, zawierających wskazanie częstotliwości audytów, sposobu przygotowywania i zatwierdzania ich planów, sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników.
3. Określi i sformalizuje procedury działań korygujących w przypadku niezgodności z wymaganiami systemu zarządzania bezpieczeństwem informacji z elementami ciągłości działania.
4. Określi i sformalizuje procedury wprowadzania działań zapobiegawczych, w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemu zarządzania bezpieczeństwem informacji.
5. Określi i sformalizuje procedury przeglądu systemu zarządzania bezpieczeństwem informacji w szczególności określającej częstotliwość przeglądów, zakres i sposób ich przeprowadzania, materiały źródłowe niezbędne do przeprowadzenia przeglądu, tryb wdrażania wniosków.
6. Określi i sformalizuje procedury nadzoru nad dokumentami wchodzącymi w skład systemu zarządzania bezpieczeństwem informacji.
7. Określi i sformalizuje procedury nadzoru nad zapisami, określające zasady/zapisy/wymagania przechowywania, archiwizowania oraz niszczenia zapisów.
8. Określi i sformalizuje procedury zarządzania ryzykiem informacyjnym, przeprowadzenie oceny ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych przez organizację zgodnie z wytycznymi aktualnej normy PN ISO/IEC 27005 wraz z przygotowaniem planu postępowania z ryzykiem zawierający m.in.:
9. zdefiniowanie sposobu pomiaru ryzyka w oparciu o rekomendacje aktualnej normy PN-ISO/IEC 27005
10. zdefiniowanie i opisanie procesu zarządzania ryzykiem
11. zdefiniowanie i opisanie inwentaryzacji aktywów informacyjnych lub grup aktywów informacyjnych zgodnie z normą PN-ISO/IEC 27005
12. zdefiniowanie i opisanie katalogu zagrożeń i oszacowanie prawdopodobieństw ich występowania
13. zdefiniowanie i opisanie identyfikacji ryzyka, szacowanie ryzyk, rejestr ryzyk
14. zdefiniowanie i opisanie planu postępowania z ryzykami.

W ramach określenia i opisu zabezpieczeń dla wymagań systemu bezpieczeństwa informacji zostaną opracowane formalne dokumenty, możliwym wykorzystaniem opisów zawartych w PN EN/ISO IEC 27002:2022, Narodowych Standardach Cyberbezpieczeństwa jako źródło tzw. stosowanych praktyk dla opracowywanych dokumentów jako zasady/zapisy/wymagania dla:

**Obszaru 1: Zabezpieczeń organizacyjnych**

1. Polityka bezpieczeństwa informacji
2. Role i obowiązki w zakresie bezpieczeństwa informacji
3. Podział obowiązków
4. Odpowiedzialności kierownictwa
5. Kontakt z organami władzy
6. Kontakt z grupami szczególnego interesu
7. Analiza zagrożeń
8. Bezpieczeństwo informacji w zarządzaniu projektami
9. Rejestr informacji i innych powiązanych zasobów
10. Dopuszczalne wykorzystanie informacji i innych powiązanych zasobów
11. Zwrot zasobów
12. Klasyfikacja informacji
13. Oznakowanie informacji
14. Transfer informacji
15. Kontrola dostępu
16. Zarządzanie tożsamością
17. Informacje uwierzytelniające
18. Prawa dostępu
19. Bezpieczeństwo informacji w relacjach z dostawcami
20. Uwzględnianie bezpieczeństwa informacji w umowach z dostawcami
21. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjnych i komunikacyjnych (ICT)
22. Monitorowanie, przegląd i zarządzanie zmianami w usługach dostawców
23. Bezpieczeństwo informacji przy korzystaniu z usług w chmurze
24. Planowanie i przygotowanie zarządzania incydentami bezpieczeństwa informacji
25. Ocena i decyzje dotyczące zdarzeń związanych z bezpieczeństwem informacji
26. Reagowanie na incydenty związane z bezpieczeństwem informacji
27. Wyciąganie wniosków z incydentów bezpieczeństwa informacji
28. Gromadzenie dowodów z naruszeń/incydentów związanych z bezpieczeństwem informacji
29. Bezpieczeństwo informacji w czasie zakłóceń związanych z bezpieczeństwem informacji
30. Gotowość technologii informacyjno- komunikacyjnych do zapewnienia ciągłości działania z elementami ISO 22301
31. Wymagania prawne, ustawowe, regulacyjne i umowne związanych z bezpieczeństwem informacji
32. Prawa własności intelektualnej
33. Ochrona zapisów
34. Prywatność i ochrona danych osobowych (PII)
35. Niezależny przegląd bezpieczeństwa informacji
36. Zgodność z polityką, zasadami i normami dotyczącymi bezpieczeństwa informacji
37. Udokumentowane procedury operacyjne

**Obszaru 2: Zabezpieczeń zasobów ludzkich**

1. Screening
2. Zasady i warunki zatrudnienia
3. Świadomość, edukacja i szkolenie w zakresie bezpieczeństwa
4. Postępowanie dyscyplinarne w konsekwencji naruszeń/incydentów związanych z bezpieczeństwem informacji
5. Obowiązki po rozwiązaniu lub zmianie zatrudnienia
6. Umowy o poufności lub nieujawnianiu informacji
7. Praca zdalna
8. Raportowanie zdarzeń dotyczących bezpieczeństwa informacji

**Obszaru 3: Zabezpieczeń fizycznych**

1. Strefy bezpieczeństwa fizycznego
2. Dostęp fizyczny
3. Zabezpieczanie biur, pomieszczeń i obiektów
4. Monitorowanie bezpieczeństwa fizycznego
5. Ochrona przed zagrożeniami fizycznymi i środowiskowymi
6. Praca w obszarach chronionych
7. Czyste biurko i czysty ekran
8. Rozmieszczenie i ochrona urządzeń
9. Bezpieczeństwo zasobów poza siedzibą firmy/organizacji
10. Nośniki danych
11. Urządzenia wspomagające
12. Bezpieczeństwo okablowania
13. Konserwacja sprzętu
14. Bezpieczna utylizacja lub ponowne wykorzystanie sprzętu

**Obszaru 4: Zabezpieczeń technologicznych**

1. Urządzenia końcowe użytkownika
2. Prawa uprzywilejowanego dostępu
3. Ograniczenie dostępu do informacji
4. Dostęp do kodu źródłowego
5. Bezpieczne uwierzytelnianie
6. Zarządzanie wydajnością
7. Ochrona przed złośliwym oprogramowaniem
8. Zarządzanie lukami technicznymi
9. Zarządzanie konfiguracją
10. Usuwanie informacji
11. Maskowanie danych
12. Zapobieganie wyciekom danych
13. Kopia zapasowa informacji
14. Nadmiarowość urządzeń do przetwarzania informacji
15. Rejestrowanie zdarzeń
16. Monitorowanie działań
17. Synchronizacja zegarów
18. Użycie uprzywilejowanych programów narzędziowych
19. Instalacja oprogramowania na systemach operacyjnych
20. Bezpieczeństwo sieci
21. Bezpieczeństwo usług sieciowych
22. Rozdzielenie sieci
23. Filtrowanie stron internetowych
24. Zastosowanie kryptografii
25. Cykl życia oprogramowania (SDLC)
26. Wymagania dotyczące bezpieczeństwa aplikacji
27. Architektura i zasady inżynierii bezpiecznych systemów
28. Bezpieczne kodowanie
29. Testy bezpieczeństwa w fazie rozwoju i akceptacji
30. Zlecone prace rozwojowe
31. Oddzielenie środowisk rozwojowych, testowych i produkcyjnych
32. Zarządzanie zmianą
33. Dane testowe
34. Ochrona systemów informatycznych podczas audytu

W przypadku stwierdzenia w trakcie opracowania wymaganych dokumentów jako zasady/zapisy/wymagania dane zabezpieczenie z w/w listy nie jest stosowane w organizacji Wykonawca przedstawia dodatkowy dokument w postaci raportu wykluczeń zabezpieczeń z dokładnym i precyzyjnym uzasadnieniem odstąpienia z opracowania wymagań dla takiego zabezpieczenia opisującym źródło takiej decyzji.

**Wymagania dla zespołu audytowo-konsultacyjnego dla realizacji obu etapów**

Zadania audytowe obu etapów będą realizowane przez min. 3 audytorów posiadających wykazane poniżej uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa z minimalnym wymaganiem dla minimalnie trzy-osobowego zespołu audytowego, gdzie:

* jedna osoba z zespołu musi posiadać certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji wg normy ISO 27001 oraz wg normy ISO 22301 w akredytacji osobowej (Dz.U.2018.1999 z 2018.10.18, Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338) oraz certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji wg normy ISO 27001 w akredytacji osobowej (Dz.U.2018.1999 z 2018.10.18, Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338)
* jedna osoba z zespołu musi posiadać certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji wg normy ISO 27001 w akredytacji osobowej (Dz.U.2018.1999 z 2018.10.18 Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338)

oraz

* jedna osoba z zespołu musi posiadać certyfikat audytora wiodącego lub wewnętrznego wg normy ISO 27701
* pozostałe dowolne certyfikaty wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r

Zamawiający wymaga minimum trzy-osobowego zespołu audytowego spełniającego powyższe warunki, lecz nie ogranicza wielkości zespołu wskazanego do realizacji przedmiotu zamówienia poprzez innych audytorów posiadających uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa.

**Doświadczenie wykonawcy**

Wykonawca musi wykazać, że skutecznie przeprowadził min. 10 audytów cyberbezpieczeństwa w tym min. 5 audytów w organizacjach będących Operatorem Usługi Kluczowej.

Wykonawca musi wykazać, że skutecznie przeprowadził min. 10 opracowań systemu SZBI, w tym min. 5 w organizacjach będących Operatorem Usługi Kluczowej.

**Kryteria Oceny i wyboru:**

1. Cena 60 pkt.
2. Kryterium Skrócenie terminu realizacji zamówienia 40 pkt.

Skrócenie termin max 5 dni kalendarzowych.

Ocena Suma

Max. 100 pkt.

**Dodatkowe ustalenia**

1. **Przedmiotowa dokumentacja nie będzie objęta prawami autorskimi Wykonawcy, a Zamawiający będzie ją mógł udostępnić jednostkom podległym biorącym udział w projekcie „Cyberbezpieczny Samorząd” w celu wykorzystania do aktualizacji przedmiotowej dokumentacji w ww. jednostkach.**
2. **Zamawiający wymaga gwarancji na aktualizację i poprawę opracowania w okresie 12 miesięcy od daty odbioru, potwierdzonego stosownym protokołem odbioru.**
3. **Wykonawcą będzie zobowiązany podpisać Umowa powierzenia**   
   **przetwarzania danych osobowych w związku z realizacja przedmiotu zamówienia.**