

Załącznik Nr 2 do Rozeznania rynku – Opis przedmiotu zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA

Wykonanie audytów zgodności z KRI-UoKSC wraz z aktualizacją/opracowaniem dokumentacji SZBI w ramach projektu pn.: „Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego”

1. Przedmiotem zamówienia jest wykonanie audytów zgodności z KRI-UoKSC wraz z aktualizacją/opracowaniem dokumentacji SZBI dla jednostek organizacyjnych Powiatu Ostrowieckiego objętych wsparciem w ramach realizowanego projektu, tj. Starostwa Powiatowego, Powiatowego Urzędu Pracy oraz Powiatowego Centrum Pomocy Rodzinie pod kątem zapewnienia cyberbezpieczeństwa.
2. Realizacja przedmiotu zamówienia obejmuje:
 - 1) Aktualizację Systemu Zarządzania Bezpieczeństwem Informacji dla Starostwa Powiatowego,
 - 2) Wykonanie audytu zgodności z KRI-UoKSC wraz z aktualizacją Systemu Zarządzania Bezpieczeństwem Informacji dla Powiatowego Urzędu Pracy,
 - 3) Wykonanie audytu zgodności z KRI-UoKSC wraz z opracowaniem Systemu Zarządzania Bezpieczeństwem Informacji dla Powiatowego Centrum Pomocy Rodzinie.
3. Przedmiot zamówienia należy wykonać zgodnie z dokumentacją oraz wytycznymi konkursu grantowego „Cyberbezpieczny Samorząd”, dostępną pod linkiem: <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad>
4. Prace wymagające udziału pracowników jednostek objętych przedmiotem zamówienia muszą być realizowane w godzinach pracy jednostek.
5. Wykonawca przedstawi szczegółowy program realizacji zamówienia dla każdej z jednostek w terminie do 7 dni roboczych od podpisania umowy oraz skonsultuje go z wyznaczonymi przedstawicielami Zamawiającego.
6. Przedmiot zamówienia musi spełniać normy i przepisy zawarte w:
 - 1) KRI (Krajowe Ramy Interoperacyjności)
 - 2) PBI (Polityka bezpieczeństwa informacji)
 - 3) SZBI (System Zarządzania Bezpieczeństwem Informacji)
 - 4) NIS (Dyrektywa NIS-1, NIS-2)
 - 5) UoKSC (Ustawa o Krajowym Systemie Cyberbezpieczeństwa)
 - 6) RODO (Ogólne rozporządzenie o ochronie danych osobowych)
 - 7) ISO 27001:22 (międzynarodowa norma standaryzująca systemy zarządzania bezpieczeństwem informacji (SZBI)).
7. 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.
8. 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) 2018/1772 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.

9. W ramach wymagań od wykonawcy, przewiduje się posiadanie zintegrowanego systemu zarządzania obejmującego certyfikaty PN-EN ISO/IEC 27001:2023 lub równoważny Międzynarodowy ISO/IEC 27001:2022.
10. W celu zapewnienia maksymalnego poziomu bezpieczeństwa informacji, wszelkie analizy i wywiady powinny być przeprowadzane na miejscu w jednostkach objętych przedmiotem zamówienia. W wyjątkowych sytuacjach, po weryfikacji wniosku Wykonawcy oraz uzyskaniu pisemnej zgody Zamawiającego, dopuszcza się formę zdalną.
11. W zamówieniu muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępność dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn. Jakikolwiek produkty (w tym dokumentacja) muszą być zgodne z zasadami uniwersalnego projektowania oraz standardami równościowymi, w szczególności ze standardem cyfrowym. Dokumentacja musi być dostosowana do potrzeb osób z niej korzystających (np. posiadać możliwość powiększania treści), jeśli występują wśród nich osoby ze szczególnymi potrzebami. Jeśli potrzeby takie nie wystąpią, Zamawiający dopuszcza dostarczenie kompletu materiałów w formacie PDF.
9. Termin wykonania:
Zamawiający wyznacza termin realizacji przedmiotu zamówienia wraz z wdrożeniem dokumentacji SZBI w jednostkach objętych wsparciem w terminie do dnia **30.11.2025 r.**, zakończonej końcowym protokołem odbioru z wcześniejszym wglądem do dokumentacji przez przedstawicieli Zamawiającego.
10. Dostarczenie dokumentacji przez wykonawcę:
 - 1) w formie papierowej, osobiście w siedzibach poszczególnych jednostek objętych przedmiotem zamówienia, tj. Starostwa Powiatowego, Powiatowego Urzędu Pracy oraz Powiatowego Centrum Pomocy Rodzinie,
 - 2) w formie elektronicznej, osobiście w siedzibach poszczególnych jednostek objętych przedmiotem zamówienia, tj. Starostwa Powiatowego, Powiatowego Urzędu Pracy oraz Powiatowego Centrum Pomocy Rodzinie, na nośniku zaszyfrowanym pendrive format plików PDF lub DOC (sposób szyfrowania i termin po uzgodnieniu z przedstawicielami Zamawiającego).
11. Na wszystkie usługi Wykonawca udzieli gwarancji wynoszącej **24 miesiące** od daty podpisania protokołu odbioru, polegającej na wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji dokumentacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w okresie gwarancji.
12. Produktem realizacji zamówienia ma być kompletna dokumentacja, będąca przedmiotem zamówienia dla poszczególnych jednostek objętych zamówieniem.
13. Wymaganie dla audytora:
Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001. Zamawiający wymaga, aby Audytor posiadał minimum

2 letnie doświadczenie w przeprowadzaniu audytów bezpieczeństwa, w tym przeprowadził minimum 2 audyty, które obejmowały zgodność z kryteriami zawartymi w § 20 ust. 2 lub § 19 ust. 2 rozporządzenia Rady Ministrów z dnia odpowiednio 12 kwietnia 2012 r. lub 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;

14. Warunki udziału w postępowaniu:

- 1) Zamawiający wymaga od Wykonawcy posiadania niezbędnej wiedzy oraz doświadczenia w zakresie objętym zamówieniem, a także dysponowania odpowiednimi osobami zdolnymi do realizacji zamówienia.
- 2) Zgodnie z Regulaminem Konkursu Grantowego pn. "Cyberbezpieczny Samorząd" audytor realizujący przedmiot zamówienia powinien posiadać odpowiednie doświadczenie oraz kwalifikacje poświadczone przynajmniej jednym z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. poz. 1999).
- 3) Wymaganie dla audytora:
Zamawiający wymaga, aby Wykonawca dysponował co najmniej jedną osobą realizującą usługę będącą przedmiotem zamówienia, która posiada co najmniej jeden z certyfikatów wymienionych w w/w ustawie oraz posiadającą co najmniej 2-letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa informacji dla jednostek administracji publicznej, w tym przeprowadził minimum 2 audyty, które obejmowały zgodność z kryteriami zawartymi w § 20 ust. 2 lub § 19 ust. 2 rozporządzenia Rady Ministrów z dnia odpowiednio 12 kwietnia 2012 r. lub 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.
- 4) Wykonawca musi posiadać oraz mieć wdrożony w organizacji certyfikat PN-EN ISO/IEC 27001:2023 lub równoważny Międzynarodowy ISO/IEC 27001:2022.

16. **Szczegółowe wymagania odnośnie przedmiotu zamówienia w zakresie poszczególnych jednostek organizacyjnych:**

16.1. Aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji dla Starostwa Powiatowego

Minimalne składowe dokumentacji:

1. Polityka Bezpieczeństwa Informacji zawierająca:
 - 1.1 Procedura i instrukcje prowadzenia audytów wewnętrznych
 - 1.2 Procedura nadzoru nad dokumentami
 - 1.3 Procedura i instrukcja działań korygujących
 - 1.4 Procedura postępowania z incydentami
 - 1.5 Polityka zarządzania zasobami ludzkimi
2. Pozostała dokumentacja SZBI:
 - 2.1 Pomiar efektywności zarządzania bezpieczeństwem informacji
 - 2.2 Deklaracja stosowania zabezpieczeń według normy iso/iec 27001
 - 2.3 Inwentaryzacja aktywów i ich właścicieli oraz zabezpieczeń
 - 2.4 Funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji (Przegląd stosowanych zabezpieczeń i dokumentów)

- 2.5 Wykaz pracowników
- 2.6 Analiza ryzyka (przeprowadzanie analizy + raport)
- 2.7 Metodyka szacowania i zarządzania ryzykiem
- 2.8 Plan ciągłości działania
3. Instrukcja zarządzania systemami informatycznymi w tym instrukcje:
 - 3.1 Instrukcja korzystania z urządzeń mobilnych
 - 3.2 Instrukcja pracy zdalnej
 - 3.3 Instrukcja eksploatacji sprzętu informatycznego
 - 3.4 Procedura kontroli dostępu
 - 3.5 Instrukcja przydzielania i odbierania dostępów użytkownikom
 - 3.6 Instrukcja przydzielania dostępów administracyjnych
 - 3.7 Polityka haseł
 - 3.8 Polityka czystego biurka i ekranu
 - 3.9 Polityka stosowania zabezpieczeń kryptograficznych
 - 3.10 Polityka kopii zapasowych
 - 3.11 Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania
 - 3.12 Instrukcja wykonywanie przeglądów i konserwacji systemów informatycznych
 - 3.13 Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym
 - 3.14 Procedura nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym
 - 3.15 Zasady korzystania z poczty elektronicznej
 - 3.16 Minimalne wymagania bezpieczeństwa dla systemów informatycznych
4. Wzory dokumentów:
 - 4.1 Rejestr zmian
 - 4.2 Karta przeglądu dokumentacji
 - 4.3 Program audytów wewnętrznych
 - 4.4 Harmonogram audytów wewnętrznych
 - 4.5 Karta audytu wewnętrznego
 - 4.6 Ewidencja wydanych aktywów
 - 4.7 Powołanie audytora
 - 4.8 Powołanie ASI
 - 4.9 Plan audytu wewnętrznego dla stacji roboczej
 - 4.10 Informacja o zarejestrowanych incydentach
5. Dokumenty związane z systemem ochrony danych osobowych:
 - 5.1 Polityka bezpieczeństwa danych osobowych
 - 5.2 Instrukcja postępowania z incydem bezpieczeństwa
 - 5.3 Procedura postępowania w sytuacji naruszenia ochrony danych osobowych
 - 5.4 Rejestr incydentów
 - 5.5 Rejestr umów powierzania danych
 - 5.6 Wniosek o udostępnienie danych osobowych
 - 5.7 Rejestr udostępnionych danych osobowych
 - 5.8 Upoważnienie do przetwarzania danych osobowych
 - 5.9 Oświadczenie o zachowaniu tajemnicy
 - 5.10 Ewidencja osób upoważnionych do przetwarzania danych osobowych

- 5.11 Wykaz miejsc przetwarzania danych osobowych
- 5.12 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania
- 5.13 Opis struktury zbiorów danych osobowych
- 5.14 Sposób przepływu danych osobowych
- 5.15 Opis ośrodków technicznych i organizacyjnych
- 5.16 Wzór- powołanie IOD
- 5.17 Wzór- umowa o zachowanie poufności i zakazie konkurencji
- 5.18 Szkolenie - listy obecności, oświadczenia pracowników
- 5.19 Rejestr Czynności Przetwarzania
- 5.20 Rejestr Kategorii Czynności przetwarzania
- 5.21 Ocena skutków dla ochrony danych/Analiza ryzyka
6. Miejscem realizacji zamówienia jest siedziba Starostwa Powiatowego w Ostrowcu Świętokrzyskim, ul. Iłżecka 37, 27-400 Ostrowiec Św.
7. Wykonawca zobowiązuje się do przeglądu i aktualizacji oraz uzupełnienia obecnych polityk o minimalne składowe. Wykonawca jest zobowiązany do przeprowadzenia aktualizacji i wdrożenia kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) dla Zamawiającego.
8. Pozostałe wymagania zgodne z opisem wskazanym powyższej części załącznika.
9. Produktem realizacji zamówienia ma być kompletna dokumentacja SZBI dla Starostwa Powiatowego w Ostrowcu Świętokrzyskim.

16.2 Wykonanie audytu zgodności z KRI-UoKSC wraz z aktualizacją Systemu Zarządzania Bezpieczeństwem Informacji dla Powiatowego Urzędu Pracy

W ramach zamówienia, należy wykonać audyt zgodności z KRI/ UoKSC oraz przegląd i aktualizację dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.

1. Audyt KRI/uoKSC

Przedmiotem zamówienia jest przeprowadzenie Audytu KRI/uoKSC.

Wykonanie audytu dokumentacji, audytu fizycznego i środowiskowego oraz audytu teleinformatycznego, a następnie przedstawienie przeprowadzonego audytu w formie raportu. Audyt obejmie całość sprzętu informatycznego Powiatowego Urzędu Pracy w Ostrowcu Św., w tym:

- Serwery fizyczne: 5
- Maszyny wirtualne: 14
- Komputery klienckie: 80
- Urządzenia UTM: 1
- Active Directory: tak

1.1 Zakres audytu KRI i uoKSC

Audyt pod kątem zgodności z wymogami KRI i uoKSC powinien uwzględniać specyficzne wymagania obu aktów prawnych, ze szczególnym naciskiem na cyberbezpieczeństwo, zarządzanie ryzykiem, reagowanie na incydenty oraz ochronę systemów informatycznych.

1.2 Audyt Dokumentacji

- 1) Ocena zgodności istniejącego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) z obowiązującymi przepisami i normami.
- 2) Audyt procedur i instrukcji wdrożonych w zakresie bezpieczeństwa informacji.
- 3) Weryfikacja regulacji wewnętrznych Zamawiającego, w tym procedur audytów i aktualizacji, pod kątem zgodności z KRI i uoKSC.
- 4) Doradztwo w zakresie uzupełnienia lub poprawy dokumentacji SZBI, obejmujące:
 - a) Omówienie obowiązków wynikających z SZBI,
 - b) Wskazanie koniecznych uzupełnień dokumentacji przez Zamawiającego.
- 5) Weryfikacja odpowiedzialności i uprawnień pracowników w obszarze bezpieczeństwa informacji, zgodnie z SZBI oraz uoKSC, wraz z odpowiednimi szkoleniami i certyfikacją.
- 6) Analiza dokumentacji dotyczącej bezpieczeństwa informacji w kontekście umów serwisowych i wykonawczych, z uwzględnieniem odpowiednich klauzul ochrony danych.
- 7) Weryfikacja aktualności i zgodności spisu sprzętu i oprogramowania wykorzystywanego do przetwarzania informacji.
- 8) Ocena analizy ryzyka oraz środków zaradczych w obszarze integralności, dostępności i poufności informacji zgodnie z wymogami KRI i uoKSC.

1.3 Audyt fizyczny i środowiskowy

- 1) Weryfikacja granic obszaru bezpiecznego zgodnie z KRI, obejmująca fizyczne granice miejsc przetwarzania danych wrażliwych oraz analizę funkcjonalności zabezpieczeń fizycznych.
- 2) Analiza zabezpieczeń dostępu do pomieszczeń, w tym systemów kontroli dostępu.
- 3) Ocena zabezpieczeń fizycznych urządzeń i pomieszczeń, obejmująca dostępność systemów monitoringu i alarmowych zgodnych z KRI.
- 4) Weryfikacja metod zabezpieczania informacji przed ujawnieniem, modyfikacją lub zniszczeniem, obejmująca sieć wewnętrzną, komputery, laptopy.
- 5) Ocena zabezpieczeń przed utratą danych, obejmująca systemy podtrzymania zasilania i chłodzenia, zgodnie z wymogami KRI.

1.4 Audyt teleinformatyczny

- 1) Weryfikacja zgodności procedur zarządzania systemami teleinformatycznymi z uoKSC i KRI, obejmująca procedury aktualizacji, monitorowania oraz reagowania na incydenty.
- 2) Przegląd zasobów informatycznych i rozwiązań w zakresie zapewnienia ciągłości działania.
- 3) Ocena procedur zarządzania aktualizacjami oprogramowania, zgodnie z wymogami KRI, z uwzględnieniem automatyzacji i monitorowania procesu.
- 4) Weryfikacja zabezpieczeń stacji roboczych.
- 5) Weryfikacja polityki haseł w zakresie zgodności z KRI i uoKSC, obejmująca wymagania dotyczące tworzenia, przechowywania i zmiany haseł.

1.5 Dokumentacja po audytowa

Po zakończeniu audytu Wykonawca przygotowuje raport zawierający:

- 1) **Wprowadzenie:** Cel, zakres, kluczowe obszary audytowane, datę przeprowadzenia audytu oraz opis objętych audytem systemów, procedur i obszarów.
- 2) **Opis zastosowanych metod i działań audytowych.**

- 3) **Ocenę zgodności z przepisami:** Ogólna ocena zgodności z uoKSC, KRI oraz innymi regulacjami (np. RODO, ISO 27001).
- 4) **Identyfikację niezgodności:** Wskazanie obszarów niezgodnych z wymogami prawnymi lub procedurami wewnętrznymi, z klasyfikacją (np. krytyczna, wysoka, średnia, niska).
- 5) **Wyniki audytu:**
 - a) Opis mocnych stron, w których Urząd spełnia wymogi i stosuje dobre praktyki w zakresie zarządzania bezpieczeństwem informacji,
 - b) Wskazanie słabych punktów, takich jak podatności, niezgodności lub braki w procedurach i zabezpieczeniach technicznych i organizacyjnych.
 - c) Ocenę ryzyka – analizę ryzyk związanych z integralnością, poufnością i dostępnością informacji oraz systemów.
- 6) **Rekomendacje i zalecenia audytorów:**
 - a) Zalecane działania naprawcze (np. wzmocnienie polityk bezpieczeństwa, poprawa procedur reagowania na incydenty, dostosowanie zabezpieczeń),
 - b) Priorytetyzacja działań (krytyczne, pilne, zalecane), umożliwiającą organizacji skuteczne planowanie działań naprawczych w celu zapewnienia zgodności.
 - c) Przedstawienie i omówienie na spotkaniu z Kierownictwem Urzędu rekomendacji i zaleceń po audytowych.
- 7) **Podpisy i oświadczenia audytorów** dotyczące rzetelności przeprowadzonego audytu i pełnego przedstawienia wyników oraz wniosków.
- 8) **Załączniki:** Lista uczestników audytu, przeanalizowanych dokumentów, polityk i procedur.

2. Przegląd i aktualizacja dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do wykonania przeglądu i aktualizacji dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) z uwzględnieniem planowanych do poniesienia nakładów w ramach grantu, a w szczególności z uwzględnieniem wykorzystania zakupywanego sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa. Powiatowy Urząd Pracy w Ostrowcu Św. jest zobowiązany do ochrony informacji w organizacji. Aktualizacja, opracowanie i wdrożenie SZBI pozwoli określić zestaw polityk, procedur, procesów, narzędzi i kompetencji, które wspomogą zwiększyć poziom cyberbezpieczeństwa.

2.1. Wykonawca zobowiązuje się do przeglądu i aktualizacji oraz uzupełnienia obecnych polityk o minimalne składowe. Wykonawca jest zobowiązany do przeprowadzenia aktualizacji i wdrożenia kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) dla Zamawiającego.

2.2. Pozostałe wymagania zgodne z opisem wskazanym w powyższej części załącznika.

2.3. Produktem realizacji zamówienia ma być kompletna dokumentacja SZBI dla Powiatowego Urzędu Pracy w Ostrowcu Św.

2.4. Dokumenty pomocne przy realizacji zamówienia obowiązujące w Urzędzie:

- 1) Zakres Systemu Zarządzania Bezpieczeństwem Informacji w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 2) Polityka Systemu Zarządzania Bezpieczeństwem Informacji w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.

- 3) Polityka zarządzania zmianami w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 4) Regulamin bezpiecznego korzystania z systemów informatycznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 5) Polityka ciągłości działania w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 6) Polityka monitorowania systemów informatycznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 7) Polityka ochrony kryptograficznej w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 8) Polityka serwisu i konserwacji systemów informatycznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 9) Polityka szkoleń z zakresu bezpieczeństwa informatycznego w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 10) Polityka współpracy z podmiotami zewnętrznymi Powiatowego Urzędu Pracy w Ostrowcu Świętokrzyskim.
- 11) Polityka wymiany informacji z wykorzystaniem systemów informatycznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 12) Polityka zabezpieczeń fizycznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 13) Procedura zarządzania ryzykiem informatycznym w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 14) Polityka zarządzania dostępem do systemów informatycznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 15) Polityka zarządzania personelem wchodzącym w skład służb informatycznych Powiatowego Urzędu Pracy w Ostrowcu Świętokrzyskim.
- 16) Polityka zarządzania pojemnością systemów informatycznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 17) Polityka zarządzania usługami informatycznymi w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 18) Procedura zarządzania pojemnością systemów informatycznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 19) Procedura instalacji oprogramowania w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 20) Procedura zarządzania incydentami w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 21) Procedura nadawania uprawnień do wstępu do pomieszczeń technicznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 22) Procedura odbierania uprawnień do wstępu do pomieszczeń technicznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 23) Procedura reagowania na podatności w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 24) Procedura serwisu i konserwacji systemów informatycznych PUP Ostrowiec Świętokrzyski w siedzibie Powiatowego Urzędu Pracy w Ostrowcu Świętokrzyskim.

- 25) Procedura serwisu i konserwacji systemów informatycznych PUP Ostrowiec Świętokrzyski poza siedzibą Powiatowego Urzędu Pracy w Ostrowcu Świętokrzyskim.
- 26) Procedura tworzenia nowego hasła do systemów informatycznych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 27) Procedura wycofywania oprogramowania w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 28) Procedura wycofywania sprzętu IT z użycia w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 29) Procedura zarządzania incydentami bezpieczeństwa w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 30) Procedura identyfikacji wymagań w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 31) Plan awaryjny reakcji na incydenty ciągłości działania w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 32) Polityka bezpieczeństwa informacji w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 33) Protokół z przeglądu dokonanego przez kierownictwo Powiatowego Urzędu Pracy w Ostrowcu Świętokrzyskim.
- 34) Procedura zarządzania ryzykiem w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 35) Deklaracja stosowania w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.
- 36) Procedura działań naprawczych w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.

2.5 Dokumentacja po aktualizacji dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Po zakończeniu aktualizacji (SZBI) Wykonawca przygotowuje raport zawierający:

- 1) Wprowadzenie: Cel, zakres, kluczowe obszary podlegające aktualizacji (SZBI), zakres dat przeprowadzenia aktualizacji.
- 2) Opis zastosowanych metod i działań.
- 3) Ocenę zgodności z przepisami: Ogólna ocena zgodności z uoKSC, KRI oraz innymi regulacjami (np. RODO, ISO 27001).
- 4) Wyniki aktualizacji (SZBI).
- 5) Zakres aktualizacji SZBI.
- 6) Opis, co konkretnie zostało zaktualizowane.
- 7) Najważniejsze wnioski z aktualizacji SZBI.
- 8) Wskazanie istotnych ryzyk, zmian lub wymagań do wdrożenia.
- 9) Podpisy i oświadczenia audytorów dotyczące rzetelności przeprowadzonego aktualizacji (SZBI) i pełnego przedstawienia wyników oraz wniosków.

2.6 Wykonawca przedstawi i omówi wykonaną aktualizację dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) na spotkaniu z Kierownictwem Urzędu, rekomendacje i wskazanie istotnych ryzyk, zmian lub wymagań do wdrożenia w organizacji.

3. Wymagania ogólne dotyczące realizacji audytu zgodności z KRI/ UoKSC oraz aktualizacji SZBI w Powiatowym Urzędzie Pracy w Ostrowcu Świętokrzyskim.

3.1. Miejscem realizacji zamówienia jest siedziba Powiatowego Urzędu Pracy w Ostrowcu Św., Aleja 3 Maja 36, 27-400 Ostrowiec Św.

3.2. **Pozostałe wymagania zgodne z opisem wskazanym w powyższej części załącznika.**

16.3 Wykonanie audytu zgodności z KRI-UoKSC wraz z opracowaniem Systemu Zarządzania Bezpieczeństwem Informacji dla Powiatowego Centrum Pomocy Rodzinie

Przedmiotem zamówienia jest przeprowadzenie audytu zgodności z KRI/UoKSC oraz opracowanie SZBI w Powiatowym Centrum Pomocy Rodzinie w Ostrowcu Świętokrzyskim.

1. Audyt KRI/UoKSC

Przedmiotem zamówienia jest przeprowadzenie Audytu KRI/UoKSC.

Wykonanie audytu dokumentacji, audytu fizycznego i środowiskowego oraz audytu teleinformatycznego, a następnie przedstawienie przeprowadzonego audytu w formie raportu. Audyt obejmie całość sprzętu informatycznego Powiatowego Centrum Pomocy Rodzinie w Ostrowcu Świętokrzyskim w tym:

- Serwery fizyczne: 2
- Maszyny wirtualne: 9
- Komputery klienckie: 56
- Urządzenia UTM: 1
- Active Directory: tak

1.1. Zakres audytu KRI i uoKSC

Audyt pod kątem zgodności z wymogami KRI i UoKSC powinien uwzględniać specyficzne wymagania obu aktów prawnych, ze szczególnym naciskiem na cyberbezpieczeństwo, zarządzanie ryzykiem, reagowanie na incydenty oraz ochronę systemów informatycznych.

1.2. Audyt fizyczny i środowiskowy

- 1) Weryfikacja granic obszaru bezpiecznego zgodnie z KRI, obejmująca fizyczne granice miejsc przetwarzania danych wrażliwych oraz analizę funkcjonalności zabezpieczeń fizycznych.
- 2) Analiza zabezpieczeń dostępu do pomieszczeń, w tym systemów kontroli dostępu.
- 3) Ocena zabezpieczeń fizycznych urządzeń i pomieszczeń, obejmująca dostępność systemów monitoringu i alarmowych zgodnych z KRI.
- 4) Weryfikacja metod zabezpieczania informacji przed ujawnieniem, modyfikacją lub zniszczeniem, obejmująca sieć wewnętrzną, komputery, laptopy.
- 5) Ocena zabezpieczeń przed utratą danych, obejmująca systemy podtrzymania zasilania i chłodzenia, zgodnie z wymogami KRI.

1.3. Audyt teleinformatyczny

- 1) Weryfikacja zgodności procedur zarządzania systemami teleinformatycznymi z uoKSC i KRI, obejmująca procedury aktualizacji, monitorowania oraz reagowania na incydenty.

- 2) Przegląd zasobów informatycznych i rozwiązań w zakresie zapewnienia ciągłości działania.
- 3) Ocena procedur zarządzania aktualizacjami oprogramowania, zgodnie z wymogami KRI, z uwzględnieniem automatyzacji i monitorowania procesu.
- 4) Weryfikacja zabezpieczeń stacji roboczych.
- 5) Weryfikacja polityki haseł w zakresie zgodności z KRI i uoKSC, obejmująca wymagania dotyczące tworzenia, przechowywania i zmiany haseł.

1.4. Dokumentacja po audytowa

Po zakończeniu audytu Wykonawca przygotowuje raport zawierający:

- 1) **Wprowadzenie:** Cel, zakres, kluczowe obszary audytowane, datę przeprowadzenia audytu oraz opis objętych audytem systemów, procedur i obszarów.
- 2) **Opis zastosowanych metod i działań audytowych.**
- 3) **Ocenę zgodności z przepisami:** Ogólna ocena zgodności z uoKSC, KRI oraz innymi regulacjami (np. RODO, ISO 27001).
- 4) **Identyfikację niezgodności:** Wskazanie obszarów niezgodnych z wymogami prawnymi lub procedurami wewnętrznymi, z klasyfikacją (np. krytyczna, wysoka, średnia, niska).
- 5) **Wyniki audytu:**
 - a) Opis mocnych stron, w których jednostka spełnia wymogi i stosuje dobre praktyki w zakresie zarządzania bezpieczeństwem informacji,
 - b) Wskazanie słabych punktów, takich jak podatności, niezgodności lub braki w procedurach i zabezpieczeniach technicznych i organizacyjnych.
 - c) Ocenę ryzyka – analizę ryzyk związanych z integralnością, poufnością i dostępnością informacji oraz systemów.

1.5. Rekomendacje i zalecenia audytorów:

- 1) Zalecane działania naprawcze (np. wzmocnienie polityk bezpieczeństwa, poprawa procedur reagowania na incydenty, dostosowanie zabezpieczeń),
- 2) Priorytetyzację działań (krytyczne, pilne, zalecane), umożliwiającą organizacji skuteczne planowanie działań naprawczych w celu zapewnienia zgodności.
- 3) Przedstawienie i omówienie na spotkaniu z Kierownictwem jednostki rekomendacji i zaleceń po audytowych.

1.6. Podpisy i oświadczenia audytorów dotyczące rzetelności przeprowadzonego audytu i pełnego przedstawienia wyników oraz wniosków.

1.7. Załączniki: Lista uczestników audytu, przeanalizowanych dokumentów, polityk i procedur.

2. Opracowanie dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do wykonania opracowania dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) z uwzględnieniem planowanych do poniesienia nakładów w ramach grantu, a w szczególności z uwzględnieniem wykorzystania zakupywanego sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa. Powiatowe Centrum Pomocy Rodzinie w Ostrowcu Świętokrzyskim jest zobowiązane do ochrony informacji w organizacji. Opracowanie i wdrożenie SZBI pozwoli określić zestaw polityk, procedur,

procesów, narzędzi i kompetencji, które wspomogą zwiększyć poziom cyberbezpieczeństwa.

2.1. Wykonawca zobowiązuje się do przeglądu i aktualizacji oraz uzupełnienie obecnych polityk o wymagane przepisami składowe. Wykonawca jest zobowiązany do przeprowadzenia opracowania i wdrożenia kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) dla Zamawiającego.

2.2. Pozostałe wymagania zgodne z opisem wskazanym w powyższej części załącznika.

2.3. Produktem realizacji zamówienia ma być kompletna dokumentacja SZBI dla Powiatowego Centrum Pomocy Rodzinie w Ostrowcu Świętokrzyskim.

2.4. Dokumenty pomocne przy realizacji zamówienia obowiązujące w jednostce:

1) Polityka ochrony danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Ostrowcu Świętokrzyskim.

2.5. Po zakończeniu opracowania (SZBI) Wykonawca prześle Zamawiającemu opracowane dokumenty i procedury w wersji papierowej jak i elektronicznej.

2.6. Wykonawca przedstawi i omówi opracowane dokumenty i procedury Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) na spotkaniu z Kierownictwem jednostki, rekomendacje i wskazanie istotnych ryzyk, zmian lub wymagań do wdrożenia w organizacji.

3. Wymagania ogólne dotyczące realizacji audytu zgodności z KRI/UoKSC oraz opracowaniem SZBI w Powiatowym Centrum Pomocy Rodzinie w Ostrowcu Świętokrzyskim.

3.1 Miejscem realizacji zamówienia jest siedziba Powiatowego Centrum Pomocy Rodzinie w Ostrowcu Świętokrzyski, ul. Świętokrzyska 22, 27-400 Ostrowiec Świętokrzyski.

3.2 Pozostałe wymagania zgodne z opisem wskazanym w powyższej części załącznika.