Załącznik nr 1

Szczegółowy opis przedmiotu zamówienia

I. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest kompleksowy przegląd, aktualizacja oraz wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (zwane dalej SZBI) zgodnie z wymaganiami Krajowych Ram Interoperacyjności (zwane dalej KRI), Ustawy o Krajowym Systemie Cyberbezpieczeństwa (zwane dalej UoKSC) oraz normy PN-EN ISO/IEC 27001:2023 – Technika informatyczna – Systemy zarządzania bezpieczeństwem informacji.
2. Zakres prac obejmuje Starostwo Powiatowe w Rzeszowie oraz jego jednostki podległe, tj. Powiatowe Centrum Pomocy Rodzinie w Rzeszowie i Zarząd Dróg Powiatowych w Rzeszowie.
3. Celem realizacji zamówienia jest podniesienie poziomu bezpieczeństwa cyfrowego Powiatu Rzeszowskiego oraz jego jednostek organizacyjnych, poprzez dostosowanie polityk, procedur i mechanizmów zabezpieczeń do obowiązujących standardów i najlepszych praktyk w zakresie zarządzania bezpieczeństwem informacji. Zamówienie jest realizowane w ramach projektu grantu pn. „*Zwiększenie poziomu bezpieczeństwa cyfrowego Powiatu Rzeszowskiego oraz jego jednostek podległych*” współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa.
4. Przedmiot zamówienia składa się z 3 (trzech) części, w tym:
   Część 1: świadczenie usługi polegającej na przeglądzie, aktualizacji i wdrożeniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Starostwa Powiatowego w Rzeszowie;
   Część 2: świadczenie usługi polegającej na przeglądzie, aktualizacji i wdrożeniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Zarządu Dróg Powiatowych w Rzeszowie;
   Część 3: świadczenie usługi polegającej na przeglądzie, aktualizacji i wdrożeniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Powiatowego Centrum Pomocy Rodzinie w Rzeszowie.
5. Przedmiot zamówienia realizowany będzie w 5 (pięciu) etapach:
   1) Etap I – Przegląd SZBI- analiza, audyt początkowy;

2) Etap II – Planowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);
3) Etap III – Inwentaryzacja i szacowanie ryzyka SZBI;
4) Etap IV – Opracowanie niezbędnej dokumentacji SZBI;
5) Etap V – Szkolenie dotyczące SZBI.

6. Wykonawca zobowiązuje się wykonać przedmiot zamówienia w terminie 180 dni od daty podpisania umowy w odniesieniu do wszystkich części i etapów zamówienia z uwzględnieniem:

1) realizacja Etapu I w terminie do 60 dni od daty podpisania umowy;
2) realizacja Etapu II w terminie do 60 dni od daty podpisania umowy;
3) realizacja Etapu III w terminie do 90 dni od daty podpisania umowy;
4) realizacja Etapu IV w terminie do 150 dni od daty podpisania umowy;
5) realizacja Etapu V w terminie do 180 dni od daty podpisania umowy.

II. Charakterystyka Zamawiającego

1. Zamówienie będzie realizowane na rzecz Starostwa Powiatowego w Rzeszowie i jednostek podległych: Powiatowego Centrum Pomocy Rodzinie w Rzeszowie oraz Zarządu Dróg Powiatowych w Rzeszowie, zwanych dalej Jednostkami.

Dane jednostek, dla których należy przygotować SZBI:

LP	Nazwa	Adres
1	Starostwo Powiatowe w Rzeszowie, w tym następujące lokalizacje:	ul. Grunwaldzka 15, 35-959 Rzeszów ul. Bernardyńska 7, 35-069 Rzeszów ul. 8 Marca 13 ul. Rynek 2, Dynów ul. Rzeszowska 29a, Sokołów Młp.,
2	Powiatowe Centrum Pomocy Rodzinie w Rzeszowie	ul. Lucjana Siemieńskiego 18a, 35-234 Rzeszów
3	Zarząd Dróg Powiatowych w Rzeszowie	ul. Budziwojska 149, 35-317 Rzeszów

2. Ogólna charakterystyka Jednostek.

2.1 Starostwo Powiatowe w Rzeszowie:

2.1.1 Starostwo Powiatowe w Rzeszowie jest jednostką sektora finansów publicznych-samorządu terytorialnego. Realizuje

2.1.2 Starostwo realizuje zadania określone w art. 4 ustawy o samorządzie powiatowym.

2.1.3 Liczba pracowników: 246

2.1.4 Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe np. drukarki, routery, przełączniki, Acces Pointy, urządzenia VoIP itp.): 743, w tym:
- ilość komputerów (również przenośnych) – 205 szt.
- ilość serwerów (fizycznych i wirtualnych): 72
    - serwery fizyczne centralne: 11 szt.
    - serwery wirtualne: 61 szt.
- ilość pozostałych urządzeń podłączonych do sieci: 466 szt.

2.1.4 Ilość podsieci: 26
2.1.6 Ilość serwerowni: 6
2.1.7 Wdrożone Active Directory: TAK
2.2. Powiatowe Centrum Pomocy Rodzinie
2.2.1 Powiatowe Centrum Pomocy Rodzinie w Rzeszowie jest jednostką organizacyjną Powiatu Rzeszowskiego.
2.2.2 PCPR realizuje zadania z zakresu pomocy społecznej, wspierania rodziny i systemu pieczy zastępczej, przeciwdziałania przemocy w rodzinie oraz rehabilitacji społecznej osób niepełnosprawnych.
2.2.3 Liczba pracowników: 52
2.2.4 Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe np. drukarki, routery, przełączniki, Acces Pointy, urządzenia VoIP itp.), w tym:
- ilość komputerów (również przenośnych) - 52 szt.
- ilość serwerów (fizycznych i wirtualnych):
    - serwery fizyczne centralne: 1 szt.
    - serwery wirtualne: 5 szt.

2.2.5 Ilość podsieci: 2
2.2.6 Ilość serwerowni: 1
2.2.7 Wdrożone Active Directory: TAK
2.3 Zarząd Dróg Powiatowych
2.3.1 Zarząd Dróg Powiatowych w Rzeszowie jest jednostką organizacyjną Powiatu Rzeszowskiego.
2.3.2 ZDP realizuje zadania związane z planowaniem, budową, modernizacją, utrzymaniem i ochroną dróg powiatowych.
2.3.3 Liczba pracowników: 30

2.3.4 Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe np. drukarki, routery, przełączniki, Acces Pointy, urządzenia VoIP itp.), w tym:

- ilość komputerów (również przenośnych) - 38 szt.
- ilość serwerów (fizycznych i wirtualnych):
  - serwery fizyczne centralne: 2 szt.
  - serwery wirtualne: 4 szt.
  - serwery NAS: 2 szt.
  - AP: 1 szt.
  - Routery: 1 szt.
  - Przełączniki: 3 szt.
- ilość central telefonicznych (VoIP): 1 szt.
- ilość telefonów IP (VoIP): 1 szt.
- ilość wideobramofonów IP (VoIP): 1 szt.
- ilość rejestratorów CCTV NVR: 1 szt.
- ilość kamer IP: 11 szt.
- ilość systemów SSWiN: 1 szt.

2.3.6 Ilość podsieci: 10

2.3.6 Ilość serwerowni: 1

2.3.7 Wdrożone Active Directory: TAK

III. Ogólne warunki realizacji zamówienia:

1. Wykonawca jest odpowiedzialny za przeprowadzenie aktualizacji i wdrożenie kompletnego SZBI dla Zamawiającego dla JST i jednostek podległych.
2. W ramach zadania wymaga się opracowania i wdrożenia następującą dokumentację:
   1) Polityka bezpieczeństwa informacji, dostosowana do wymogów ISO 27001 oraz przepisów krajowych.
   2) Procedury operacyjne SZBI, obejmujące m.in. zarządzanie incydentami, klasyfikację i ochronę informacji oraz zarządzanie dostępem.
   3) Analiza ryzyka, zgodna z metodyką określoną w ISO 27001 oraz wytycznymi KRI.
   4) Plan postępowania z ryzykiem, określający działania minimalizujące potencjalne zagrożenia dla bezpieczeństwa informacji.
   5) Rejestry zgodności i audytów, dokumentujące weryfikację zgodności wdrożonych rozwiązań z obowiązującymi przepisami i normami.

6) Instrukcje i wytyczne dla pracowników, podnoszące świadomość i zapewniające zgodność działań z przyjętymi standardami bezpieczeństwa.

3. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z ankietą dojrzałości cyberbezpieczeństwa wykonaną w ramach realizacji grantu i złożoną przez Zamawiającego do NASK oraz uwzględnić w ramach aktualizacji i wdrożenia SZBI planowany w Ankiecie zakres usprawnień SZBI.
4. 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.

IV. Zakres przedmiotu zamówienia:

Celem usługi jest aktualizacja i wdrożenie procedur systemów zarządzania bezpieczeństwem informacji funkcjonujących u Zamawiającego z uwzględnieniem uwarunkowań i specyfiki projektu oraz specyfiki jednostek. Analiza zostanie przeprowadzona zgodnie z wymogami ISO/IEC 19011:2018. 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, zasad bezpieczeństwa informacji, z metody inwentaryzacji i klasyfikacji aktywów informacyjnych, z dokumentacji ochrony informacji.
4. Aktualizacja/opracowanie Polityki Bezpieczeństwa Informacji 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) zarządzania aktywami;
   3) zarządzania zasobami ludzkimi;
   4) organizacji bezpieczeństwa fizycznego i środowiskowego;
   5) zarządzania komunikacją i eksploatacją;
   6) rejestru czynności przetwarzania i rejestr kategorii czynności przetwarzania;
   7) kontroli dostępu, zarządzania hasłami, stosowania zabezpieczeń kryptograficznych, czystego biurka i czystego ekranu, usuwania i niszczenia informacji, pracy w strefach bezpieczeństwa;
   8) akwizycji, rozwoju i utrzymania systemu;
   9) zarządzania incydentami związanymi z bezpieczeństwem informacji;
   10) zarządzania ciągłością działania;
   11) zarządzania kopiami zapasowymi;
   12) zarządzania monitoringiem;
   13) zobowiązania do zachowania poufności, stosowania polityk i procedur SZBI;
   14) używania urządzeń komputerowych;
   15) metod szacowania i postępowania z ryzykiem;
   16) deklaracji 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.

6. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedury bezpieczeństwa fizycznego obejmujące obowiązek wyznaczania osoby odpowiedzialnej za bezpieczeństwo fizyczne.
7. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedury bezpieczeństwa fizycznego obejmujące zasady ruchu materiałowego i osobowego.
8. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zasady odpowiedzialności za cyberbezpieczeństwo wraz ze wskazaniem obowiązku wyznaczania osoby odpowiedzialnej za cyberbezpieczeństwo.
9. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń z zakresu cyberbezpieczeństwa wraz z wprowadzeniem obowiązku regularnego, corocznego prowadzenia szkoleń.
10. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje treść zarządzenia wdrażającego SZBI dla Zamawiającego.
11. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzkiem obejmujący systematyczne tworzenie raportów oceny ryzyka w Jednostce oraz konieczność cyklicznego przeglądu tego raportu przez Kierownika JST.
12. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje szczegółowy sposób realizacji celów oraz we współpracy z Zamawiającym przypisze odpowiedzialności za ich realizację.
13. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedurę wprowadzającą obowiązek regularnego, corocznego przeglądu SZBI jednostki.
14. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń obejmującą obowiązek informowania o zmianach w SZBI w toku okresowych szkoleń stanowiskowych.
15. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kluczowe aktywa informacyjne Jednostki (zbiory danych/systemy/usługi).
16. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje rejestr ryzyk uwzględniający aktywa Jednostki.
17. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zagrożenia związane z cyberbezpieczeństwem w ramach procesów zarządczych oraz zarządzania ryzykiem.
18. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzkiem związanym z zagrożeniami bezpieczeństwa informacji.
19. 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.

20. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek identyfikacji i priorytetyzacji odpowiedzi na ryzyka.
21. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą system oceny ryzyka.
22. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem cyberbezpieczeństwa uwzględniającą identyfikowane, ustanawiane i oceniane ryzyka.
23. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania danymi uwzględniającą polityki ich niszczenia, plan backup, plany reagowania i odtwarzania danych.
24. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami.
25. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania zapisami zdarzeń / logów/ inspekcji.
26. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę użytkowania dostępu do odczytu lub zapisu danych z zewnętrznych nośników danych.
27. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów.
28. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami uwzględniający obowiązek dokumentowania ryzyka z nimi związanego.
29. 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 obsłużonych incydentów.
30. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów wraz z obowiązkiem ich aktualizacji.
31. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę planów odtwarzania uwzględniającą obowiązek ich aktualizacji w obszarze doświadczeń i wniosków z prowadzonych procesów odtwarzania.

V. Etapy realizacji zamówienia

ETAP I. Przegląd SZBI – analiza, audyt początkowy

W ramach Etapu I Wykonawca zobowiązany jest do:

1. Określenia stanu spełnienia wymagań prawnych nałożonych na organizację w zakresie ochrony informacji.
2. Sprawdzenia spełnienia wymagań i zaleceń w ramach standardów PN-EN ISO/IEC 27001:2023 i norm pokrewnych.
3. Inwentaryzacji aktywów informacyjnych i ocena ryzyka.
4. Oceny zabezpieczeń technicznych, organizacyjnych oraz fizycznych.
5. Analizy dokumentacji Polityki Bezpieczeństwa Informacji.
6. Analizy dokumentacji Polityki Bezpieczeństwa Danych Osobowych.
7. Opracowania zestawu działań mających na celu określenie stanu faktycznego zabezpieczeń technicznych w systemie informatycznym:

LP	Zadanie	Opis
1	Ocena schematu sieci	Topologia: Zastosowana architektura sieci (np. gwiazda, hierarchiczna, rozproszona) Podział na segmenty: Oddzielenie zasobów publicznych i wewnętrznych, strefa DMZ dla usług zewnętrznych Łącza i redundancja: Zapewnienie niezawodności działania sieci
2	Określenie rodzaju połączeń	LAN oraz WLAN - separacja ruchu administracyjnego, sieci pracowniczej i gości WAN - Połączenia z ePUAP, CEIDG, KSI ZUS, CEPiK itp. oraz MPLS VPN/IPsec VPN
3	Określenie segmentów sieci	Z podziałem dla Starostwa i osobno dla podległych JST Zasoby (inwentaryzacja aktywów + obieg dokumentacji), bezpieczeństwo (SIEM, LDAP, MFA)
4	Przeprowadzenie oceny środowiska informatycznego	Ocena poziomu eksploatacji i wsparcia dla: - serwery i systemy pamięci masowej; - sprzęt sieciowy i topologia; - połączenia pomiędzy JST i jednostkami podległymi
5	Ocena sposobu identyfikowania i logowania użytkowników	AIM; Zarządzanie uprawnieniami; Stosowanie polityki haseł

LP	Zadanie	Opis
6	Analiza zarządzania kontami użytkowników	Analiza narzędzi oraz procedury w Dziale IT; - systemy lokalne – zarządzanie; - systemy zewnętrzne – zarządzanie.
7	Analiza strony www i BIP pod kątem ochrony danych osobowych	- Stos technologiczny; - Bazy danych; - Wsparcie; - DNS oraz SSL;
8	Analiza systemu backupów i archiwizacji danych	Rodzaj backupu: pełny, różnicowy, przyrostowy Częstotliwość tworzenia kopii: codzienny backup danych operacyjnych, miesięczny backup archiwalny Lokalizacja przechowywania kopii: serwery lokalne, chmura, nośniki offline Mechanizmy szyfrowania i zabezpieczenia kopii
9	Określenie miejsc redundancji w sieci i systemach informatycznych	Analiza ruchu sieciowego dla LAN i WAN; Skuteczne przełączanie na wypadek awarii; Ocena HA.
10	Analiza konfiguracji zabezpieczeń systemów operacyjnych na serwerach	Weryfikacja wersji OS (Windows Server, linux) Aktualizowanie i patchowanie aktualności Optymalizacja usług sieciowych i otwartych portów MFA, hasła itp. Konfiguracja bezpieczeństwa w tym firewall oraz EDR/XDR
11	Analiza konfiguracji zabezpieczeń baz danych	Kontrola dostępu; Szyfrowanie danych i transmisji; Ochrona przed atakami i podatnościami (w tym zabezpieczenia pod kątem SQL Injection).
12	Określenie bezpieczeństwa aplikacji i serwerów WWW	Aktualizacje; Optymalizacja usług sieciowych; Implementacja WAF Bezpieczeństwo (XSS, CSRF, SSL itd.)
13	Analiza konfiguracji urządzeń sieciowych:	VLAN, ACL dla izolacji ruchu Zabezpieczenia sieci do interfejsów (SSH i ograniczone IP) Systemy IDS/IPS

LP	Zadanie	Opis
	switche, routery, IDS, IPS, UTM, firewall	Lista zablokowanych IP Polityki dla UTM/firewall
14	Ocena zabezpieczeń dostępu do sieci publicznej	Na poziomie LAN/WLAN, WAN Stosowanie VLAN oraz NAC
15	Badanie podatności systemów operacyjnych za pomocą specjalistycznego oprogramowania	Testy podatności dla systemów operacyjnych Symulacja cyberataków Ocena konfiguracji i rekomendacje
16	Analiza zabezpieczeń stacji roboczych	Aktualizacje OS oraz oprogramowania Weryfikacja centralnego zarządzania aktualizacjami lub wdrożenie lokalnych polityk Polityki haseł oraz MFA Weryfikacja antywirusów z EDR/XDR
17	Analiza ochrony danych na komputerach przenośnych	Szyfrowanie dysków Zabezpieczenia BIOS/UEFI MFA i biometria
18	Badanie zabezpieczeń nośników zewnętrznych	Czy jest zgoda Stosowanie szyfrowania na nośnikach zewn. Weryfikacja polityk dla nośników
19	Sprawdzenie procedur zarządzania ciągłością działania	Weryfikacja obecnego planu zarządzania ciągłości działania Określenie kluczowych systemów i procesów Przypisanie odpowiednich ról Raporty z przywracania usług Redundancja systemów i infrastruktury

8. Opracowania raportu z audytu początkowego 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.
9. Termin realizacji Etapu I: do 60 dni od daty podpisania umowy.

ETAP II. Planowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

W ramach Etapu II Wykonawca zobowiązany jest do:

1. Przeprowadzenia instruktażu dla kadry zarządzającej z zasad bezpieczeństwa informacji.
2. Określenia zakresu SZBI, w tym:
   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. Zdefiniowania wymaganych polityk SZBI, w tym:
   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, w tym:
   1) wybór metody szacowania ryzyka;
   2) określenie kryteriów akceptowalności ryzyk i identyfikacji akceptowalnych poziomów ryzyk;
   3) zdefiniowanie obszarów zabezpieczeń objętych analizą ryzyka.
5. Wyboru celów zabezpieczeń, w tym:
   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.

6. Termin realizacji Etapu II: do 60 dni od daty podpisania umowy.

ETAP III. Inwentaryzacja i szacowanie ryzyka SZBI.

W ramach Etapu III Wykonawca zobowiązany jest do:

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 początkowego;
   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.
5. Termin realizacji etapu III: do 90 dni od daty podpisania umowy.

ETAP IV. Opracowanie niezbędnej dokumentacji SZBI

W ramach Etapu IV Wykonawca zobowiązany jest do:

1. Opracowania wspólnie z pracownikami Jednostek wymaganych procedur i instrukcji, w tym:
   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. Wykonania projektu zabezpieczeń - opracowania projektu zabezpieczeń i konsultacje przy wdrożeniu odpowiednio skutecznych zabezpieczeń zgodnych z celami zabezpieczeń.
3. Opracowania programu uświadamiania i szkolenia.
4. Przeprowadzenia instruktaży dla pracowników z dokumentacji ochrony informacji.
5. Przeprowadzenia instruktaży dla kadry zarządzającej z dokumentacji ochrony informacji.
6. Termin realizacji Etapu IV: do 150 dni od daty podpisania umowy.

Etap V. Szkolenie dotyczące SZBI

W ramach Etapu V Wykonawca zobowiązany jest do:

1. Przeprowadzenia szkolenia dla wszystkich pracowników upoważnionych do przetwarzania danych osobowych w związku z wdrożeniem SZBI oraz udokumentowanie przeprowadzenia tego szkolenia.
2. Szkolenie powinno obejmować co najmniej:
   - omówienie podstawowych zasad bezpieczeństwa informacji, wynikających z SZBI i PBI,
   - odpowiedzialność za naruszenie zasad SZBI i PBI,
   - zasady zgłaszania i reagowania na incydenty.
   - szkolenia będą kierowane do wszystkich pracowników, maksymalnie 4 godziny zegarowe , szkolenia on-line, termin szkolenie będzie uzgodniony z zamawiającym po podpisaniu umowy.
3. Termin realizacji Etapu V: do 180 dni od daty podpisania umowy.