Załącznik nr 2

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Informacje ogólne. Cel zamówienia.

1. Celem usługi w ramach działania będzie aktualizacja i wdrożenie procedur systemu zarządzania bezpieczeństwem informacji wdrożonych u Zamawiającego z uwzględnieniem uwarunkowań i specyfiki projektu. 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.
2. Przedmiot zamówienia będzie realizowany w ramach projektu konkursu grantowego pn. „Cyberbezpieczny Samorząd" realizowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Priorytet II: Zaawansowane usługi cyfrowe (dalej: konkurs „Cyberbezpieczny Samorząd").
3. Opracowana w wyniku niniejszego postępowania dokumenty będą aktualizować stan bezpieczeństwa informacji, w tym zwłaszcza w kontekście zadań realizowanych w ramach konkursu „Cyberbezpieczny Samorząd" i zgodnie z dokumentami opracowanymi w ramach ww. konkursu, w tym zwłaszcza „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego", stanowiącej Załącznik nr 6 do Regulaminu konkursu Cyberbezpieczny Samorząd.

II. Szczegółowy opis przedmiotu zamówienia.

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 ryzkiem 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 obsłużonych 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: switche, 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.

Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej przez Wykonawcę dokumentacji. Wykonawca zobowiązany jest do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego.

Realizując zadanie objęte niniejszą umową Wykonawca zobowiązany jest do zapewnienia dostępności architektonicznej, cyfrowej oraz informacyjno – komunikacyjnej, osobom ze szczególnymi potrzebami, co najmniej w zakresie określonym przez minimalne wymagania, o których mowa w art. 6 ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz. U. z 2024 r. poz. 1411).

Szczegółowy harmonogram realizacji zamówienia będzie ustalany z Zamawiającym po podpisaniu umowy. Zamawiający zadba o dostępność dokumentacji potrzebnej do realizacji Przedmiotu umowy.

Na zakończenie realizacji zamówienia Wykonawca przekaże Zamawiającemu opracowane dokumenty w wersji papierowej oraz elektronicznej.