załącznik nr 2

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zaprojektowanie i wdrożenie Polityki Bezpieczeństwa Informacji oraz Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z wymaganiami normy PN-ISO/IEC 27001:2014, w Urzędzie Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych, z siedzibą w Warszawie (02-222) przy Al. Jerozolimskich 181C (dalej „Zamawiający" lub „Urząd").

I. ZAŁOŻENIA DOTYCZĄCE ZAMÓWIENIA

1. Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych Urzędu poprzez opracowanie strategicznych i szczegółowych uregulowań w zakresie bezpieczeństwa informacji oraz poprzez wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami nw. aktów prawnych, norm i wytycznych:
   a) PN-ISO/IEC 27001:2014 oraz zalecenia ujęte w: PN-ISO/IEC 27002:2014, PN-ISO/IEC 27005:2014, PN-ISO/IEC 24762:2010;
   b) 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), w skrócie „RODO";
   c) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
   d) ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
   e) ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
   f) ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej;
   g) rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (w skrócie „KRI");
   h) rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (w skrócie „rMSWiA");
   i) wszystkie inne ustawy i rozporządzenia, którym podlega Zamawiający w zakresie bezpieczeństwa informacji;
   j) wytyczne GIODO (https://www.giodo.gov.pl) dotyczące opracowania i wdrożenia polityki bezpieczeństwa.
2. Motywy powodujące konieczność realizacji zamówienia:
   a) brak zbiorczych, zunifikowanych wytycznych dla Polityki Bezpieczeństwa Informacji w Urzędzie oraz brak wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji,
   b) konieczność zestandaryzowania procedur bezpieczeństwa wynikających ze stale rosnących zasobów informacji gromadzonych w formie tradycyjnej oraz bazach danych Urzędu,
   c) konieczność podniesienia poziomu bezpieczeństwa usług udostępniania informacji z obszaru objętego właściwością Urzędu.
3. Realizacja zamówienia potencjalnie spowoduje pozytywne skutki, tj.:
   a) zapewni bezpieczeństwo danych i systemów posiadanych przez Urząd oraz powierzanych Urzędowi w oparciu o normy, akty prawne i wytyczne wymienione w pkt 1,

b) ograniczy czas niedostępności systemów informatycznych Urzędu z powodów ich awarii, poprzez opracowanie Planów Ciągłości Działania,

c) zoptymalizuje koszty utrzymania i rozwoju systemów informatycznych oraz koszty zabezpieczenia infrastruktury teleinformatycznej Urzędu przed działaniem szkodliwego oprogramowania i próbami włamań;

d) zapewni bezpieczeństwo procesu udostępniania danych,

e) ustandaryzuje rozwiązania (technologie) oraz metody budowy interfejsów.

4. Informacje ogólne o środowisku Zamawiającego:

a) Przetwarzanie informacji odbywa się w Warszawie: w siedzibie Urzędu przy Al. Jerozolimskich 181C oraz w pomieszczeniu archiwum przy ul. Przecławskiej 1. Informacje przetwarzane są w formie papierowej oraz systemach informatycznych. Zamawiający zatrudnia około 500 osób.

b) Zakres informacji gromadzonej przez Urząd, jest określony odpowiednio w:
- ustawie z dnia 18 marca 2011 r. o Urzędzie Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych;
- ustawie z dnia 6 września 2001 r. Prawo farmaceutyczne;
- ustawie z dnia 9 października 2015 r. o produktach biobójczych;
- ustawie z dnia 20 maja 2010 r. o wyrobach medycznych;
oraz aktach wykonawczych do ww. ustaw.

c) Środowisko teleinformatyczne zawiera obecnie około 650 elementów aktywnych sieci i około 80 serwerów fizycznych i wirtualnych.

5. Zamawiający w ciągu 3 dni od dnia zawarcia Umowy przekaże Wykonawcy dokumenty, którymi dysponuje w obszarze związanym z bezpieczeństwem informacji, w tym procedury wewnętrzne i wyniki przeprowadzonych audytów oraz szczegółową strukturę organizacyjną i informacje o środowisku teleinformatycznym, niezbędne do opracowania przez Wykonawcę wstępnego harmonogramu prac.

6. W przypadku, gdy w trakcie realizacji zamówienia (umowy) zmianie ulegną normy lub przepisy prawa wymienione w pkt 1 i 4, Wykonawca ma obowiązek uwzględnić te zmiany w realizowanej usłudze.

II. ZAKRES ZAMÓWIENIA

1. Podstawowe wymagania w zakresie realizacji zaprojektowania i wdrożenia Polityki Bezpieczeństwa Informacji oraz Systemu Zarządzania Bezpieczeństwem Informacji

1) Usługa zaprojektowania i wdrożenia Polityki Bezpieczeństwa Informacji (w skrócie PBI) oraz Systemu Zarządzania Bezpieczeństwem Informacji (w skrócie SZBI) będzie obejmować swoim zakresem:
- etap I - audyt przedwdrożeniowy w Urzędzie;
- etap II - szkolenia wstępne dla grupy pracowników wskazanych przez Zamawiającego i kierownictwa Urzędu;
- etap III - klasyfikacja informacji przetwarzanych w Urzędzie;
- etap IV - szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Urzędzie zgodnie z wytycznymi normy PN-ISO/IEC 27005:2014;
- etap V - opracowanie dokumentacji PBI;
- etap VI - szkolenia z zakresu PBI dla pracowników i kierownictwa Urzędu;
- etap VII - audyt powdrożeniowy.

2) Każdy etap określony w ppkt 1 podlega ocenie oraz formalnemu zaakceptowaniu przez Zamawiającego.

3) Wszelkie informacje dotyczące usługi przekazywane między Wykonawcą a Zamawiającym będą zabezpieczone przed nieuprawnionym dostępem w sposób określony przez Zamawiającego.

2. Audyt przedwdrożeniowy

1) Audyt przedwdrożeniowy ma na celu weryfikację poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2014 przez Urząd, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych w Urzędzie, w obszarach określonych załącznikiem A do ww. normy, tj.:
   - Polityki bezpieczeństwa informacji (A.5);
   - Organizacja bezpieczeństwa informacji (A.6);
   - Bezpieczeństwo zasobów ludzkich (A.7);
   - Zarządzanie aktywami (A.8);
   - Kontrola dostępu (A.9);
   - Kryptografia (A10);
   - Bezpieczeństwo fizyczne i środowiskowe (A.11);
   - Bezpieczna eksploatacja (A.12);
   - Bezpieczeństwo komunikacji (A.13)
   - Pozyskiwanie, rozwój i utrzymanie systemów (A.14);
   - Relacje z dostawcami (A.15);
   - Zarządzanie incydentami związanymi z bezpieczeństwem informacji (A.16);
   - Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania (A.17);
   - Zgodność (A.18).
2) Wykonawca zbada zgodność działań Zamawiającego z uregulowaniami prawnymi, którym podlega Urząd w zakresie bezpieczeństwa informacji, tj.:
   - RODO;
   - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
   - ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,
   - ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
   - ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej,
   - KRI,
   - rMSWiA.
3) Audyt podlega przeprowadzeniu we wszystkich komórkach organizacyjnych Urzędu, w siedzibie przy Al. Jerozolimskich 181C oraz ul. Przecławskiej 1 w Warszawie.
4) Przed rozpoczęciem prac Wykonawca przedstawi Zamawiającemu do akceptacji szczegółowy plan audytu.
5) Zakres prac audytu przedwdrożeniowego będzie obejmował co najmniej:
   - zapoznanie się ze strukturą organizacyjną Urzędu;
   - analizę i ocenę dokumentacji i systemów teleinformatycznych w zakresie bezpieczeństwa informacji, w tym polityk, procedur, zarządzeń, instrukcji oraz innych dokumentów, które Zamawiający udostępni Wykonawcy do analizy; Zamawiający zastrzega sobie prawo do udostępnienia dokumentacji tylko i wyłącznie w jego siedzibie;
   - wywiady analityczne z wyznaczonymi przez Zamawiającego pracownikami komórek organizacyjnych w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa określonych w normie PN-ISO/IEC 27001:2014 oraz wewnętrznych uregulowaniach Urzędu;
   - obserwacje budynków, pomieszczeń, działań i zachowań pracowników Urzędu;
6) Wykonawca opracuje i sporządzi raport z przeprowadzonego audytu przedwdrożeniowego, zawierający w szczególności:
   - cel i zakres audytu;

- opis przeprowadzonych prac;
- opis poziomu spełnienia każdego z wymagań normy PN-ISO/IEC 27001:2014 opisanych w załączniku A do normy;
- wykaz stwierdzonych niezgodności w odniesieniu do każdego wymagania określonego w normie PN-ISO/IEC 27001:2014 zgodnie z załącznikiem A, na poziomie opisu poszczególnych zabezpieczeń wraz z przedstawieniem dowodów na istnienie niezgodności;
- rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności w odniesieniu do każdego z wymagań normy PN-ISO/IEC 27001:2014 opisanego w załączniku A;
- podsumowanie i wnioski.

7) Raport, o którym mowa w ppkt 6, Wykonawca przekaże Zamawiającemu w formie papierowej w dwóch egzemplarzach oraz w formie elektronicznej w plikach edytowalnych w formatach docx, pptx, xlix, w postaci cyfrowego repozytorium dokumentów, zapewniającego ich wersjonowanie. Raport w formie elektronicznej Wykonawca zabezpieczy przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu na nośniku danych CD/DVD, a także prześle pocztą elektroniczną na adresy email wskazane przez Zamawiającego.
8) Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu. Wykonawca zobowiązany jest do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego.

3. Szkolenia wstępne dla pracowników Urzędu

1) Po zakończeniu audytu przedwdrożeniowego Wykonawca zobowiązany jest do przygotowania i poprowadzenia szkoleń wstępnych z zakresu PBI, przeznaczonych dla kierownictwa Urzędu oraz zespołu roboczego PBI, powołanego przez Urząd do współpracy z Wykonawcą.
2) Szkolenie dla kierownictwa Urzędu będzie swoim zakresem obejmowało co najmniej:
   - wprowadzenie do problematyki PBI;
   - wprowadzenie do zarządzania ryzykiem;
   - przedstawienie celów projektu, harmonogramu oraz oczekiwanych rezultatów na poszczególnych etapach.
3) Szkolenie dla zespołu roboczego PBI będzie swoim zakresem obejmowało co najmniej:
   - przedstawienie celów projektu, harmonogramu oraz oczekiwanych rezultatów na poszczególnych etapach;
   - omówienie wybranych wyników audytu przedwdrożeniowego;
   - omówienie wymagań normy PN-ISO/IEC 27001:2014;
   - wprowadzenie do zarządzania ryzykiem;
   - omówienie roli i obowiązków zespołu roboczego PBI w projekcie;
   - sposób komunikacji na dalszych etapach projektu między Wykonawcą a Zamawiającym.
4) Szkolenie dla kierownictwa Urzędu będzie obejmować od 2 do 4 godzin.
5) Szkolenie dla zespołu roboczego PBI będzie obejmować od 4 do 8 godzin.
6) Szkolenia dla kierownictwa Urzędu oraz zespołu roboczego PBI odbędą się w siedzibie Zamawiającego w dni robocze w godzinach 8:30-15:30.
7) Wykonawca przekaże Zamawiającemu harmonogram, materiały szkoleniowe i prezentacje w zakresie szkoleń, o których mowa w ppkt 1-6, najpóźniej na 7 dni przed planowanym terminem rozpoczęcia szkoleń.
8) Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanych przez Wykonawcę materiałów szkoleniowych oraz harmonogramu szkoleń, w tym do zmiany planowanych terminów szkoleń. Wykonawca zobowiązany jest do uwzględnienia uwag przekazanych przez Zamawiającego.

9) Wykonawca zobowiązany jest ponadto do przygotowania i przedłożenia Zamawiającemu:
   - imiennej listy obecności uczestników szkolenia, sporządzanej odrębnie dla każdego dnia szkolenia, zawierającej: informacje o liczbie godzin, obecności danej osoby, podpis uczestnika szkolenia, podpis wykładowcy/- ów;
   - ankiet oceny szkolenia, wypełnionych i podpisanych przez uczestników szkolenia.

10) Zamawiający zastrzega sobie prawo do rejestracji audiowizualnej przebiegu szkoleń.

4. Klasyfikacja informacji

1) W ramach procesu klasyfikacji informacji Wykonawca jest zobowiązany do zrealizowania następujących prac:
   - opracowanie metodyki klasyfikowania informacji przetwarzanych w Urzędzie;
   - opracowanie modelu podziału informacji przetwarzanych w Urzędzie w zależności od poziomu ich wrażliwości i przeznaczenia z uwzględnieniem informacji niejawnych;
   - przeszkolenie pracowników Urzędu w zakresie sposobu klasyfikowania informacji na bazie wcześniej opracowanej metodyki;
   - sklasyfikowanie wspólnie z pracownikami poszczególnych komórek organizacyjnych informacji przetwarzanych w Urzędzie;
   - opracowanie raportu z procesu klasyfikacji informacji.

2) Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej przez Wykonawcę metodyki klasyfikowania informacji, nie później jednak niż na 7 dni roboczych przed rozpoczęciem szkoleń pracowników Urzędu w zakresie sposobu klasyfikowania informacji. Uwagi muszą zostać uwzględnione przez Wykonawcę.

3) Dokumentację, o której mowa w ppkt 1, a w szczególności opis metodyki klasyfikowania informacji oraz raport z procesu klasyfikowania informacji Wykonawca przekaże Zamawiającemu w formie papierowej w dwóch egzemplarzach oraz w formie elektronicznej w plikach edytowalnych w formatach: docx, pptx, xlsx, w postaci cyfrowego repozytorium dokumentów, zapewniającego ich wersjonowanie. Dokumentację w formie elektronicznej Wykonawca zabezpieczy przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu na nośniku danych CD/DVD, a także prześle pocztą elektroniczną na adresy email wskazane przez Zamawiającego.

4) Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanej przez Wykonawcę dokumentacji określonej w ppkt 1. Wykonawca zobowiązany jest do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego.

5) Najważniejsze wnioski z procesu klasyfikacji informacji Wykonawca przygotuje i przedstawi na życzenie Zamawiającego w formie prezentacji multimedialnej.

5. Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Urzędzie

1) W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Urzędzie, a w szczególności:
   - opracować metodykę szacowania ryzyka spełniającą wymagania PN-ISO/IEC 27005:2014, optymalną ze względu na charakter działalności Urzędu; Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej metodyki analizy ryzyka, a Wykonawca zobowiązany jest je uwzględnić; ponadto Wykonawca zobowiązany jest do przeprowadzenia procesu szacowania ryzyka zgodnie z wybraną i zatwierdzoną przez Zamawiającego metodyką szacowania ryzyka;
   - opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk;
   - przeszkolić wybranych pracowników Urzędu w zakresie przyjętej metodyki szacowania ryzyka;
   - przeprowadzić wspólnie z wyznaczonymi pracownikami Urzędu proces szacowania ryzyka, w tym:

zinwentaryzować zasoby (aktywa informacyjne) oraz ich właścicieli, określić zagrożenia dla zasobów, określić podatności dla zasobów, określić skutki utraty poufności, integralności i dostępności zasobów oraz przeanalizować i ocenić zidentyfikowane ryzyka;
- opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Urzędu;
- opracować przy współudziale wyznaczonych pracowników Urzędu plan postępowania z ryzykiem.

2) Dokumentację, o której mowa w ppkt 1, tj. metodykę szacowania ryzyka, raport z procesu szacowania ryzyka oraz plan postępowania z ryzykiem Wykonawca przekaże Zamawiającemu w formie papierowej w dwóch egzemplarzach oraz w formie elektronicznej w plikach edytowalnych w formatach: docx, pptx, xlsx, w postaci cyfrowego repozytorium dokumentów, zapewniającego ich wersjonowanie. Dokumentację w formie elektronicznej Wykonawca zabezpieczy przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu na nośniku danych CD/DVD, a także prześle pocztą elektroniczną na adresy email wskazane przez Zamawiającego.
3) Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanej przez Wykonawcę dokumentacji określonej w ppkt 1. Wykonawca jest zobowiązany do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego.

6. Opracowanie dokumentacji Polityki Bezpieczeństwa Informacji

1) Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest opracować i przedstawić koncepcję wdrożenia Polityki Bezpieczeństwa Informacji w Urzędzie.
2) Koncepcja będzie w szczególności zawierać mapę dokumentów PBI, stanowiącą szczegółowy wykaz dokumentów PBI z zaznaczeniem ich wzajemnych powiązań, w tym:
- Dokument Główny Polityki Bezpieczeństwa Informacji definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa w proces zapewnienia bezpieczeństwa informacji, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji;
- Polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji w Urzędzie w tym dla obszaru: teleinformatycznego, danych osobowych, informacji niejawnych, innych tajemnic prawnie chronionych, zabezpieczeń fizycznych, ciągłości działania, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa. Zamawiający dopuszcza, aby w zakresie ochrony informacji niejawnych przetwarzanych zgodnie u ustawą o ochronie informacji niejawnych, dokument zawierał jedynie odwołania i odniesienia do istniejących u Zamawiającego regulacji w tym zakresie;
- Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

3) Dla każdego dokumentu, o którym mowa w ppkt 2, Wykonawca opracuje i przedstawi Zamawiającemu do akceptacji szczegółowy zakres merytoryczny.
4) W przypadku dokumentów funkcjonujących w Urzędzie, odnoszących się do bezpieczeństwa informacji, których zakres merytoryczny będzie w całości lub częściowo pokrywał się z opracowanymi przez Wykonawcę projektami dokumentów PBI, Wykonawca zaproponuje i uzasadni sposób ich, wyłączenia, zastąpienia lub zintegrowania z zaproponowaną przez Wykonawcę mapą dokumentów.
5) Wykonawca zaprojektuje organizację Systemu Zarządzania Bezpieczeństwem Informacji, uwzględniając rozwijany w Urzędzie Zintegrowany System Zarządzania Jakością.
6) Zamawiający zastrzega sobie prawo do wnoszenia uwag do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego. Uwagi wniesione przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji

wdrożenia PBI.

7) Na podstawie zatwierdzonej przez Zamawiającego koncepcji, o której mowa w pakt 1 i 2, Wykonawca opracuje wszystkie opisane w koncepcji dokumenty Polityki Bezpieczeństwa Informacji. Dokumenty PBI muszą być zgodne ze wszystkimi wymaganiami prawnymi, którymi podlega Urząd, w tym w zakresie bezpieczeństwa informacji, zgodnie z pkt 2 ppkt 2 oraz z wymaganiami normy PN-ISO/IEC 27001:2014. Jeżeli w czasie realizacji umowy wymagania prawne w zakresie bezpieczeństwa informacji ulegną zmianie, Wykonawca zobowiązany jest dostosować dokumentację PBI do zaistniałych zmian.
8) Wszystkie dokumenty Polityki Bezpieczeństwa Informacji Wykonawca przekaże Zamawiającemu w formie papierowej w dwóch egzemplarzach oraz w formie elektronicznej w plikach edytowalnych w formatach: docx, pptx, xlsx, w postaci cyfrowego repozytorium dokumentów, zapewniającego ich wersjonowanie. Dokumentację w formie elektronicznej Wykonawca zabezpieczy przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu na nośniku danych CD/DVD, a także prześle pocztą elektroniczną na adresy email wskazane przez Zamawiającego.
9) Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów PBI. Wykonawca jest zobowiązany do uwzględnienia w dokumentach PBI uwag wniesionych przez Zamawiającego.

7. Szkolenia z zakresu Polityki Bezpieczeństwa Informacji

1) Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń z zakresu Polityki Bezpieczeństwa Informacji dla pracowników Urzędu, obejmujących co najmniej:
   - omówienie podstawowych zasad bezpieczeństwa informacji, wynikających z PBI;
   - odpowiedzialność za naruszenie zasad PBI;
   - zasady zgłaszania i reagowania na incydenty.
2) Szkolenia dla pracowników zostaną przeprowadzone dla siedemnastu 30-osobowych grup; szkolenie każdej grupy będzie obejmować 7 godzin lekcyjnych w czasie jednego dnia szkolenia.
3) Wykonawca przygotuje i przeprowadzi szkolenia dla audytorów wewnętrznych i innych wyznaczonych pracowników, a także trenerów PBI.
4) Szkolenie dla audytorów wewnętrznych i innych wyznaczonych pracowników, będzie obejmować co najmniej:
   - zasady audytowania PBI;
   - monitorowanie skuteczności PBI;
   - opracowanie wyników audytu wewnętrznego.
5) Celem szkolenia dla trenerów PBI jest zdobycie przez uczestników szkolenia wiedzy, umożliwiającej prowadzenie szkoleń z zakresu PBI dla pracowników Urzędu.
6) Szkolenie dla audytorów wewnętrznych i innych wyznaczonych pracowników będzie przeprowadzone dla 10 osób, a szkolenie dla trenerów PBI dla 20 osób. Każde z ww. szkoleń będzie obejmować 14 godzin lekcyjnych, tj. po 7 godzin lekcyjnych dziennie w czasie 2 dni szkolenia.
7) Szkolenia dla wszystkich ww. grup będą odbywały się w siedzibie Zamawiającego w dni robocze w godzinach 8:30-15:30.
8) Wykonawca przekaże do akceptacji Zamawiającemu harmonogram szkoleń, materiały szkoleniowe i prezentacje najpóźniej na 14 dni przed planowanym terminem rozpoczęcia szkoleń.
9) Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanych przez Wykonawcę materiałów szkoleniowych i harmonogramu szkoleń, w tym do zmiany planowanych terminów szkoleń.

Wykonawca zobowiązany jest do uwzględnienia uwag wniesionych przez Zamawiającego.

10) Wykonawca zobowiązany jest ponadto do przygotowania i przedłożenia Zamawiającemu:
- imiennej listy obecności uczestników szkolenia sporządzanej odrębnie dla każdego dnia szkolenia, zawierającej: informacje o liczbie godzin, obecności danej osoby, podpis uczestnika szkolenia, podpis wykładowcy/-ów;
- ankiet oceny szkolenia wypełnionych i podpisanych przez uczestników szkolenia.

11) Zamawiający zastrzega sobie prawo do rejestracji audiowizualnej przebiegu szkoleń.

8. Audyt powdrożeniowy

1) Audyt powdrożeniowy obejmuje następujące prace:
- weryfikacja poziomu wdrożenia w Urzędzie zabezpieczeń zgodnie z rekomendacjami, o których mowa w pkt 2 ppkt 6;
- weryfikacja stosowania zasad określonych w Polityce Bezpieczeństwa Informacji przez pracowników Urzędu;
- ocena poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2014 zgodnie z załącznikiem A do tej normy;
- ocena zgodności z przepisami zawartymi w aktach prawnych, wymienionych w pkt 2 ppkt 2.

2) Audyt podlega przeprowadzeniu w wybranych komórkach organizacyjnych Urzędu.

3) Wykonawca przedstawi Zamawiającemu do akceptacji szczegółowy plan audytu.

4) Wykonawca opracuje raport z audytu powdrożeniowego, zawierający co najmniej:
- cel i zakres przeprowadzonego audytu;
- opis przeprowadzonych prac;
- szczegółowy opis poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2014 w obszarach, w których podczas audytu przedwdrożeniowego stwierdzono niezgodności;
- potwierdzenie spełnienia wymogów przepisów zawartych w aktach prawnych wymienionych w pkt 2 ppkt 2, w tym potwierdzenie zgodności z przepisami RODO;
- wykaz zaobserwowanych niezgodności w odniesieniu do stosowania przez pracowników Urzędu zasad polityki bezpieczeństwa informacji;
- szczegółowy opis działań korygujących i naprawczych;
- ogólną ocenę poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2014 zgodnie z załącznikiem A do tej normy oraz poziomu stosowania przez pracowników Urzędu zasad PBI;
- podsumowanie i wnioski.

5) Raport, o którym mowa w ppkt 4, Wykonawca przekaże Zamawiającemu w formie papierowej w dwóch egzemplarzach oraz w formie elektronicznej w plikach edytowalnych w formatach: docx, pptx, xlsx, w postaci cyfrowego repozytorium dokumentów, zapewniającego ich wersjonowanie. Raport w formie elektronicznej Wykonawca zabezpieczy przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu na nośniku danych CD/DVD, a także prześle pocztą elektroniczną na adresy email wskazane przez Zamawiającego.

6) Zamawiający zastrzega sobie prawo do wnoszenia uwag do raportu przekazanego przez Wykonawcę. Wykonawca jest zobowiązany do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego.

7) Najważniejsze wnioski z audytu powdrożeniowego Wykonawca jest zobowiązany przygotować i przedstawić na życzenie Zamawiającemu w formie prezentacji multimedialnej.

III. HARMONOGRAM REALIZACJI ZAMÓWIENIA

1. Termin realizacji zamówienia wynosi **7 miesięcy od dnia zawarcia umowy**. Z uwagi na konieczność dostosowania Urzędu do wymagań RODO w terminie do 25 maja 2018 r., Wykonawca zobowiązany jest do wykonania prac w tym obszarze obejmujących opracowanie kompletnej dokumentacji Polityki Bezpieczeństwa Informacji w zakresie dotyczącym ochrony danych osobowych wraz procedurami i instrukcjami stanowiącymi zestaw szczegółowych dokumentów, wynikających z ww. polityki stanowiącej element Systemu Zarządzania Bezpieczeństwem informacji w zakresie danych osobowych i przekazania Zamawiającemu ww. dokumentacji oraz przedstawienia raportu potwierdzającego zgodność z ww. wymaganiami RODO **do dnia 21 maja 2018 r.**
2. W ciągu 5 dni od dnia przekazania materiałów przez Zamawiającego po zawarciu umowy Wykonawca przedstawi i przekaże Zamawiającemu wstępny harmonogram wykonania usług. Zamawiający ma prawo do wnoszenia uwag do przedstawionego harmonogramu w terminie 7 dni od dnia otrzymania harmonogramu. Wykonawca zobowiązany jest do ich uwzględnienia w terminie 4 dni od dnia wniesienia uwag. Uzgodniony wstępny harmonogram podlega akceptacji przez Zamawiającego.
3. Przed przystąpieniem do każdego etapu prac Wykonawca opracuje i przedstawi Zamawiającemu szczegółowy harmonogram realizacji danego etapu. Rozpoczęcie prac nad danym etapem jest możliwe po zaakceptowaniu przez Zamawiającego harmonogramu szczegółowego dotyczącego danego etapu. Harmonogramy muszą zawierać terminy wykonania poszczególnych prac, w tym terminy wnoszenia i akceptacji uwag do produktów prac objętych danym etapem oraz terminy rozpoczęcia i zakończenia danego etapu.