Opis przedmiotu zamówienia

Opracowanie oraz wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI), przeprowadzenie audytu KRI oraz analizy ryzyka przetwarzania danych osobowych jednostek organizacyjnych Gminy Miasto Lubartów na potrzeby projektu „Zwiększenie cyberbezpieczeństwa Gminy Miasto Lubartów" realizowanego w ramach programu „Cyberbezpieczny samorząd",

I. OGÓLNE WARUNKI REALIZACJI ZAMÓWIENIA

1. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Zakres prac:

1) Etap I: „Polityka Bezpieczeństwa Informacji jako podstawowy element systemu zarządzania bezpieczeństwem informacji" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w w/w. obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Bezpieczeństwa Informacji;
c) przygotowanie i przekazanie Polityki Bezpieczeństwa Informacji;
d) doradztwo we wdrożeniu Polityki Bezpieczeństwa Informacji;
e) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego w obszarze przyjętej Polityki Bezpieczeństwa Informacji.

2) Etap II: „Polityka Ochrony Danych" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w ww. obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Ochrony Danych;
c) przygotowanie i przekazanie Polityki Ochrony Danych;
d) doradztwo we wdrożeniu Polityki Ochrony Danych;
e) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego obejmujące wdrożoną Politykę Ochrony Danych oraz omówienie przyjętych procedur zgodnie z przepisami z zakresu ochrony danych w oparciu o przepisy Rozporządzenia 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) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781).

3) Etap III: „Polityka Zarządzania Systemem Teleinformatycznym" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w w/w. obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Systemem Informatycznym;
c) przygotowanie i przekazanie Polityki Zarządzania Systemem Informatycznym wraz z Planami Ciągłości Działania w obszarze IT;
d) doradztwo we wdrożeniu Polityki Zarządzania Systemem Informatycznym;
e) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego obejmujące wszystkie procesy z obszaru Krajowych Ram Interoperacyjności.

4) Etap IV: „Polityka Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w w/w obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Ciągłością Działania;
c) przygotowanie i przekazanie Polityki Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT;
d) doradztwo we wdrożeniu Polityki Zarządzania Ciągłością Działania;
e) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego obejmujące obszar utrzymania ciągłości działania.

5) Etap V „Polityka Zarządzania Incydentami Cyberbezpieczeństwa" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w w/w obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Incydentami Cyberbezpieczeństwa;
c) przygotowanie i przekazanie Polityki Zarządzania Incydentami Cyberbezpieczeństwa;
d) przygotowanie i przekazanie Planu Reagowania na Incydenty;
e) przygotowanie i przekazanie Planu Zarządzania Podatnościami;
f) doradztwo we wdrożeniu dokumentacji wymienionej w ppkt c)-e);
g) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu Zamawiającego obejmujące wdrożoną Politykę Zarządzania Incydentami Cyberbezpieczeństwa oraz wymogów prawnych wynikających Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2024 r., poz. 1077).

6) Etap VI: „Analiza Ryzyka Bezpieczeństwa Informacji" obejmuje następujące czynności:

a) analiza ekspercka wyników zrealizowanego uprzednio na zasobach Zamawiającego audytu wstępnego systemu bezpieczeństwa informacji w w/w obszarze;
b) konsultacje z przedstawicielem Zamawiającego w celu przeprowadzenia analizy ryzyka;
c) przygotowanie i przekazanie Raportu z przeprowadzonej analizy ryzyka wraz z omówieniem obszarów o podniesionym ryzyku wraz z rekomendacjami.

7) Etap VII: Inne dokumenty (oprócz wymienionych w pkt. 1-6), które mają być przygotowane przez Wykonawcę lub dostosowane, w przypadku ich posiadania przez Zamawiającego:

a) procedury korzystania z urządzeń mobilnych,
b) procedury pracy zdalnej,
c) procedury kontroli dostępu,
d) zabezpieczenie pomieszczeń i obiektów,
e) procedury czystego biurka,
f) procedury czystego ekranu,
g) procedury kopii zapasowych,
h) postępowanie z nośnikami
i) procedury ochrony logów,
j) bezpieczeństwo komunikacji,
k) zarządzanie bezpieczeństwem sieci,
l) przesyłanie informacji,
m) plany ciągłości działania,
n) procedury zarządzania incydentami,
o) prywatność i ochrona danych osobowych,
p) szacowanie ryzyka w obszarze bezpieczeństwa informacji,
q) plan zarządzania podatnościami,
r) plan reagowania na incydenty,
s) plan przywracania,
t) szkolenia personelu w zakresie wdrożenia dokumentacji SZBI.

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. ANALIZA RYZYKA

Zakres:

- przegląd środków organizacyjnych i technicznych oraz istniejącej dokumentacji dotyczącej ochrony danych osobowych;
- ocena istniejących zagrożeń dla podatności, dostępności, integralności i rozliczalności danych osobowych;
- szacowanie ryzyka (ocena podatności i skutków) dla:
  - sieci teleinformatycznych,
  - serwerów baz danych (systemy i zasoby teleinformatyczne),
  - stacji dostępowych;
- ocena ryzyka i skutków przetwarzania dla zasobów (sprzęt, alarmy, monitoringi, telefony itp);
- ocena ryzyka i oceny skutków przetwarzania dla podatności, dostępności, integralności i rozliczalności danych osobowych;
- opracowanie rekomendacji;
- opracowanie tabel i dokumentacji dla klienta;
- omówienie rekomendacji i istniejącego poziomu ryzyka i dalszych działań.

3. AUDYT KRI:

Zakres i przedmiot audytu bezpieczeństwa informacji obejmuje analizę:

- zgodności procedur wewnętrznych Instytucji z zakresu zarządzania bezpieczeństwem informacji z KRI;
- aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
- inwentaryzacji sprzętu i oprogramowania;
- ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko;
- weryfikację uprawnień osób zaangażowanych w proces przetwarzania danych;
- faktu przeprowadzania szkoleń z zakresu bezpieczeństwa informacji i ochrony danych osobowych;
- ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
- zasad używania urządzeń mobilnych i pracy na odległość;
- zabezpieczeń informacji w sposób uniemożliwiający nieuprawnione ich ujawnienie, modyfikację, usunięcie lub zniszczenie;
- umów serwisowych;
- zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
- poziomu bezpieczeństwa w systemach teleinformatycznych;
- incydentów związanych z naruszeniem bezpieczeństwa informacji;
- przeprowadzania okresowych audytów wewnętrznych w zakresie bezpieczeństwa informacji.
- W ramach Audytu ma być wykonany również:
  - audyt zgodności z RODO;
  - analiza jakościowego i ilościowego wykorzystywania sprzętu komputerowego;
  - analiza podatności systemów informatycznych.

II ORGANIZACJA REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Do realizacji zamówienia Zamawiający wymaga personelu Wykonawcy posiadającego odpowiednie kwalifikacje i doświadczenie.
2. Wykonawca wyznaczy do realizacji zamówienia zespół składający się z minimum 3 osób (audytorów) a spośród nich Kierownika zespołu.

3. Kierownik zespołu będzie posiadał pełną wiedzę o realizowanym projekcie oraz będzie odpowiedzialny za komunikację w projekcie i podpisywanie raportów, przedstawianie harmonogramów oraz ewentualnych zmian.
4. Wszystkie dokumenty sporządzone będą w formie pisemnej w języku polskim, w formie papierowej lub formie elektronicznej w formacie danych .pdf lub jednym z formatów edytowalnych: .doc, .rtf, .xlsx.