Załącznik nr 2.5 do SIWZ

Gmina Dąbrówno
ul. Kościuszki 21
14-120 Dąbrówno

Szczegółowy Opis Przedmiotu Zamówienia

Część V - Opracowanie dokumentacji System Zarządzania Bezpieczeństwem Informacji (SZBI) w ramach projektu pn. "Zintegrowany system świadczenia e-usług publicznych Gminy Dąbrówno".

Dąbrówno, grudzień 2021

SPIS TREŚCI

1.0. Przedmiot zamówienia

Przedmiotem zamówienia jest Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w ramach projektu pn. "Zintegrowany system świadczenia e-usług publicznych Gminy Dąbrówno".

1.1. Wymagania prawne

Oferowane przez Wykonawcę rozwiązania muszą być na dzień odbioru zgodne z aktami prawnymi regulującymi pracę urzędów administracji publicznej oraz usług urzędowych realizowanych drogą elektroniczną. Oferowane rozwiązania muszą być zgodne w szczególności z następującymi przepisami (z ich późniejszymi zmianami):

1. Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2021 r., poz. 1372)
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781) – dalej „UODO"
3. 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) – dalej „RODO"
4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
5. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2020 poz. 344).
6. Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. 2015 poz. 1341)
7. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2021 poz. 670)
8. Rozporządzenie Rady Ministrów z dnia 6 października 2016 r. zmieniające rozporządzenie w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz.U. 2016 poz. 1634)
9. 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 (Dz.U. 2017, poz. 2247) – dalej „RKRI"
10. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2019 poz. 848)
11. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz. 1560) – dalej „UKSC"

2.0. Opracowanie dokumentacji System Zarządzania Bezpieczeństwem Informacji (SZBI)

Na usługę opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji składają się:

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. Raport powinien opisywać tematyczne obszary zabezpieczeń wynikające z Załącznika A do Normy ISO/IEC 27001, wraz zaleceniami do wdrożenia dla zapewnienia zgodności z wymaganiami prawnymi w zakresie ochrony informacji, tj. RODO, UODO, RKRI oraz UKSC.
3. Opracowanie projektu dokumentacji SZBI z dokumentem nadrzędnym - Polityki Bezpieczeństwa Informacji oraz politykami szczegółowymi, instrukcjami i procedurami wynikającymi z wymagań

prawnych oraz dobrych praktyk w odniesieniu do norm bezpieczeństwa informacji. Dokumentacja SZBI musi być zgodna z wymogami przepisów RODO, UODO, RKRI oraz UKSC i obejmować co najmniej następujące obszary:

- organizacja systemu bezpieczeństwa informacji;
- zarządzanie aktywami;
- zarządzanie zasobami ludzkimi;
- organizacja bezpieczeństwa fizycznego i środowiskowego;
- zasady komunikacji i eksploatacji;
- zarządzanie kontrolą dostępu;
- zarządzanie zmianami;
- zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- zarządzanie ciągłością działania.

4. Wdrożenie Polityki Bezpieczeństwa Informacji. Poprzez wdrożenie należy rozumieć 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.

Poszczególne etapy realizacji usługi.

Etap I. Audyt zerowy.

1. Określenie stanu spełnienia wymagań prawnych w zakresie ochrony informacji, tj. RODO, UODO, RKRI oraz UKSC oraz dobrych praktyk wynikających z normy PN-ISO/IEC 27001.
2. Ocena zabezpieczeń technicznych, organizacyjnych oraz fizycznych.
3. Analiza spełnienia wymagań paragrafu 20 RKRI, RODO, UODO oraz UKSC z uwzględnieniem analizy strony www i BIP
4. Analiza dokumentacji SZBI, w tym Polityki Bezpieczeństwa Informacji i powiązanych polityk, instrukcji, procedur i regulaminów.
5. 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 w zakresie ochrony informacji, zasad wiedzy technicznej i dobrych praktyk wynikających z normy PN-ISO/IEC 27001.

Etap II. Diagnoza Cyberbezpieczeństwa

1. 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) Określenie miejsc redundancji w sieci i systemach informatycznych.
   7) Analiza konfiguracji zabezpieczeń systemów operacyjnych na serwerach.
   8) Analiza konfiguracji zabezpieczeń baz danych.
   9) Określenie bezpieczeństwa aplikacji i serwerów WWW.

10) Analiza konfiguracji urządzeń sieciowych: switche, routery, IDS, IPS, UTM, firewall.
11) Ocena zabezpieczeń dostępu do sieci publicznej.
12) Badanie podatności systemów operacyjnych za pomocą specjalistycznego oprogramowania.
13) Analiza zabezpieczeń stacji roboczych.

Etap III. Inwentaryzacja i szacowanie ryzyka SZBI.

1. Inwentaryzacja aktywów oraz przypisanie do grup aktywów.
2. Ocena i analiza zagrożeń, skutków i prawdopodobieństwa wystąpienia.
3. Zdefiniowanie planów postępowania z ryzykiem.
4. Opracowanie raportu z szacowania ryzyka.

Etap IV. 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 V. Opracowanie niezbędnej dokumentacji SZBI.

1. Opracowanie dla zamawiającego dokumentacji SZBI, w tym:
   1) opracowanie Polityki Bezpieczeństwa Informacji;
   2) opracowanie Polityk szczegółowych, np. Danych Osobowych;
   3) opracowanie Instrukcji Zarządzania Systemem Informatycznym;
   4) opracowanie procedury zarządzania zmianami, w tym w odniesieniu do zasad privacy-by-design i privacy-by-default;
   5) opracowanie procedury zarządzania incydentami;
   6) opracowanie planów awaryjnych na wypadek naruszenia ciągłości działania;
2. Przeprowadzenie szkoleń dla pracowników z dokumentacji SZBI i bezpieczeństwa informacji.

Zamawiający zastrzega, że opracowanie dokumentacji SZBI powinno rozpocząć się w ciągu 7 dni od wezwania Wykonawcy do realizacji zakresu zadań opisanego w niniejszym punkcie. Zamawiający zastrzega, że opracowanie dokumentacji SZBI powinno dotyczyć tylko elementów wynikających z realizacji niniejszego przedmiotu zamówienia.

Zamawiający żąda udzielenia gwarancji na opracowanie dokumentacji SZBI na okres minimum 24 miesięcy:

1. W ramach udzielonej gwarancji Wykonawca zobowiązuje się do usunięcia wszelkich nieprawidłowości (błędów) w opracowanej dokumentacji SZBI zidentyfikowanych po terminie odbioru dokumentacji. Usunięcie nieprawidłowości (błędów) w opracowanej dokumentacji nastąpi w terminie nie dłuższym niż 14 dni od dnia zgłoszenia przez Zamawiającego nieprawidłowości (błędów) pisemnie bądź za pomocą poczty elektronicznej.
2. W ramach udzielonej gwarancji Wykonawca zobowiązuje się do dostosowania i aktualizacji opracowanej dokumentacji SZBI do zmian środowiska Zamawiającego oraz wymagań prawnych w terminie nie dłuższym niż 14 dni od dnia przekazania przez Zamawiającego zgłoszenia. Zamawiający dokonuje zgłoszenia, o którym mowa w niniejszym ustępie drogą pisemną bądź za pomocą poczty

elektronicznej.

3. W ramach udzielonej gwarancji Wykonawca zobowiązuje się do dostarczania poprawionej dokumentacji SZBI, dostosowania i aktualizacji opracowanej dokumentacji SZBI do zmian środowiska Zamawiającego oraz wymagań prawnych.