Projekt „Cyfrowa gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2022. Sfinansowano w ramach reakcji Unii na pandemię COVID-19.

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zaprojektowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji oraz Polityki Bezpieczeństwa Informacji, zgodnie z wymaganiami normy PN-ISO/IEC 27001:2017, w Urzędzie Miasta Gorzowa Wielkopolskiego.

1. ZAŁOŻENIA

Celem wdrożenia 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 27001:2017,
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 - 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) 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").

2. TERMIN REALIZACJI

Całościowa realizacja zamówienie nastąpi do 8 (ośmiu) miesięcy od daty zawarcia umowy.

3. ZAKRES PRAC

Usługa zaprojektowania i wdrożenia Polityki Bezpieczeństwa Informacji (w skrócie PBI) oraz Systemu Zarządzania Bezpieczeństwem Informacji (w skrócie SZBI) będzie obejmować swoim zakresem:

a) Etap I - audyt przedwdrożeniowy w Urzędzie;
b) Etap II - szkolenie wstępne dla kadry zarządzającej oraz grupy pracowników wskazanych przez Zamawiającego;
c) Etap III – opracowanie projektu SZBI;
d) Etap IV - Wdrożenie SZBI:
   - klasyfikacja informacji przetwarzanych w Urzędzie;
   - szkolenie wszystkich pracowników Zamawiającego (e-learning – 2 x 4 godziny);
   - analiza ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Urzędzie;
   - pomoc w opracowaniu dokumentacji PBI;
e) Etap V – przygotowanie audytów wewnętrznych;

f) Etap VI – przygotowanie przeglądu zarządzania;
g) Etap VII – uczestnictwo w audycie certyfikującym.

Każdy etap podlega ocenie oraz formalnemu zaakceptowaniu przez Zamawiającego. Wszelkie informacje dotyczące usługi przekazywane między Wykonawcą, a Zamawiającym będą zabezpieczone przed nieuprawnionym dostępem w sposób określony przez Zamawiającego.

4. AUDYT PRZEDWDROŻENIOWY

1. Audyt przedwdrożeniowy ma na celu weryfikację poziomu spełnienia wymagań normy PN-ISO/IEC 27001 przez Urząd, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych w Urzędzie, w obszarach określonych Załącznikiem A do ww. normy, tj.:
   a) Polityki bezpieczeństwa informacji (A.5);
   b) Organizacja bezpieczeństwa informacji (A.6);
   c) Bezpieczeństwo zasobów ludzkich (A.7);
   d) Zarządzanie aktywami (A.8);
   e) Kontrola dostępu (A.9);
   f) Kryptografia (A10);
   g) Bezpieczeństwo fizyczne i środowiskowe (A.11);
   h) Bezpieczna eksploatacja (A.12);
   i) Bezpieczeństwo komunikacji (A.13)
   j) Pozyskiwanie, rozwój i utrzymanie systemów (A.14);
   k) Relacje z dostawcami (A.15);
   l) Zarządzanie incydentami związanymi z bezpieczeństwem informacji (A.16);
   m) Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania (A.17);
   n) Zgodność (A.18).
2. W ramach audytu przedwdrożeniowego Wykonawca przeprowadzi diagnozę cyberbezpieczeństwa zgodnie z zakresem oraz formularzem stanowiącym Załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina zakończonego raportem. Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący Załącznik nr 8 konkursu grantowego załączony do niniejszego Zaproszenia do złożenia oferty.
3. O udzielenie niniejszego zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki, Programu Cyfrowa Gmina tj.:
   Audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu znajduje się poniżej:
   a) Certified Internal Auditor (CIA);
   b) Certified Information System Auditor (CISA);

Projekt „Cyfrowa gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2022. Sfinansowano w ramach reakcji Unii na pandemię COVID-19.

c) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
d) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
e) Certified Information Security Manager (CISM);
f) Certified in Risk and Information Systems Control (CRISC);
g) Certified in the Governance of Enterprise IT (CGEIT);
h) Certified Information Systems Security Professional (CISSP);
i) Systems Security Certified Practitioner (SSCP);
j) Certified Reliability Professional;
k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

4. Przed rozpoczęciem prac Wykonawca uzgodni z Zamawiającym szczegółowy plan audytu.
5. Zakres prac audytu przedwdrożeniowego będzie obejmował co najmniej:
   a) zapoznanie się ze strukturą organizacyjną Urzędu;
   b) 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;
   c) wywiady analityczne z wyznaczonymi przez Zamawiającego pracownikami komórek organizacyjnych w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa określonych w normie PN-ISO/IEC 27001:2017 oraz wewnętrznych uregulowaniach Urzędu;
   d) weryfikację stosowanych w Urzędzie zabezpieczeń teleinformatycznych zgodnie
   z pkt. 1;
   e) analizę podziału stref bezpiecznych budynków i pomieszczeń;
   f) analizę działań i zachowań pracowników Urzędu;
6. Produktem tego etapu prac będzie opracowany i sporządzony przez Wykonawcę raport z przeprowadzonego audytu przedwdrożeniowego, zawierający w szczególności:
   a) cel i zakres audytu;
   b) opis przeprowadzonych prac;
   c) opis poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2017 opisanych w Załączniku A do normy;
   d) wykaz stwierdzonych niezgodności w odniesieniu do wymagań określonych w normie PN-ISO/IEC 27001:2017 zgodnie z załącznikiem A, na poziomie opisu poszczególnych zabezpieczeń;

e) rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności w odniesieniu do wymagań normy PN-ISO/IEC 27001:2017 opisanych w załączniku A zgodnie z pkt. 1;
f) podsumowanie i wnioski;
g) wypełniony formularz stanowiący Załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina (https://www.gov.pl/web/cppc/cyfrowa-gmina).

7. Raport 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.
8. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu. Wykonawca zobowiązany jest do odniesienia się w raporcie do uwag wniesionych przez Zamawiającego.

5. SZKOLENIA WSTĘPNE

1) Szkolenie dla kadry zarządzającej Zamawiającego (szkolenie stacjonarne 2 godziny).
2) Po zakończeniu audytu przedwdrożeniowego Wykonawca zobowiązany jest do przygotowania i poprowadzenia szkoleń wstępnych z zakresu PBI, przeznaczonych dla zespołu roboczego, powołanego przez Urząd do współpracy z Wykonawcą.
3) Szkolenie dla zespołu roboczego (2 x 4 godziny, on-line) będzie swoim zakresem obejmowało co najmniej:
   a) przedstawienie celów projektu, harmonogramu oraz oczekiwanych rezultatów na poszczególnych etapach;
   b) omówienie wybranych wyników audytu przedwdrożeniowego;
   c) omówienie wymagań normy PN-ISO/IEC 27001:2017;
   d) wprowadzenie do zarządzania ryzykiem;
   e) omówienie roli i obowiązków zespołu roboczego PBI w projekcie;
   f) sposób komunikacji na dalszych etapach projektu między Wykonawcą a Zamawiającym.
4) Wykonawca zobowiązany jest ponadto do przygotowania i przedłożenia Zamawiającemu:
   a) 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;
   b) ankiet oceny szkolenia, wypełnionych i podpisanych przez uczestników szkolenia.
5) Produktem tego etapu prac będzie:
   a) Imienna lista przeszkolonych osób;
   b) Uzgodniony z Zamawiającym plan szkoleń;

c) Materiały szkoleniowe przekazane w formie elektronicznej Zamawiającemu oraz uczestnikom szkolenia w najpóźniej dzień przed rozpoczęciem szkolenia, sporządzone w języku polskim;
d) Ankiety oceny szkolenia wypełnione przez uczestników szkolenia, mające na celu zebranie informacji na temat jakości szkolenia;
e) Imienne zaświadczenie o ukończeniu szkolenia wydane każdemu uczestnikowi szkolenia wydane przez Wykonawcę po zakończeniu szkolenia,
f) Protokół potwierdzający pozytywne potwierdzenie zrealizowania szkolenia podpisany przez strony.

6. KLASYFIKACJA INFORMACJI

1) W ramach procesu klasyfikacji informacji Wykonawca jest zobowiązany do zrealizowania następujących prac:
   a) opracowanie metodyki klasyfikowania informacji przetwarzanych w Urzędzie;
   b) opracowanie modelu podziału informacji przetwarzanych w Urzędzie w zależności od poziomu ich wrażliwości i przeznaczenia (bez informacji niejawnych);
   c) przeszkolenie zespołu roboczego w zakresie sposobu klasyfikowania informacji
   na bazie wcześniej opracowanej metodyki;
   d) sklasyfikowanie wspólnie z pracownikami poszczególnych komórek organizacyjnych informacji przetwarzanych w Urzędzie;
   e) opracowanie raportu z procesu klasyfikacji informacji.
2) Produktem tego etapu prac będzie:
   a) Uzgodniona z Zamawiającym metodyka klasyfikacji i ochrony informacji,
   b) Szkolenie zespołu roboczego w zakresie sposobu klasyfikowania informacji
   na bazie wypracowanej metodyki,
   c) Raport z klasyfikacji informacji podpisany przez strony.

7. ANALIZA RYZYKA

1) W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych
   w Urzędzie, a w szczególności:
   a) opracować metodykę szacowania ryzyka, optymalną ze względu na charakter działalności Urzędu; Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej metodyki analizy ryzyka, a Wykonawca zobowiązany jest je rozpatrzyć;
   b) 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;

c) opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Urzędu;
d) opracować przy współudziale wyznaczonych pracowników Urzędu plan postępowania z ryzykiem.

2) Dokumentację, 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.
3) Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanej przez Wykonawcę proponowanej dokumentacji, a Wykonawca jest zobowiązany
do rozpatrzenia uwag wniesionych przez Zamawiającego.
4) Produktem tego etapu prac będzie:
a) Uzgodniona z Zamawiającym metodyka szacowania ryzyka;
b) Szkolenie zespołu roboczego w zakresie sposobu szacowania ryzyka na bazie wypracowanej metodyki;
c) Raport z szacowania ryzyka podpisany przez strony;
d) Plan postępowania z ryzykiem uzgodniony z Zamawiającym.

8. OPRACOWANIE DOKUMENTACJI

1) Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest opracować wspólnie z zespołem roboczym Zamawiającego 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:
3) 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;
4) Polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji w Urzędzie w tym dla obszaru: teleinformatycznego, danych osobowych, 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.
5) Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.
6) 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, Wykonawca zaproponuje i uzasadni sposób ich włączenia lub

Projekt „Cyfrowa gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2022. Sfinansowano w ramach reakcji Unii na pandemię COVID-19.

zintegrowania
z zaproponowaną przez Wykonawcę mapą dokumentów.

7) 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 rozpatrzone przez Wykonawcę.
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.
9) Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany
do rozpatrzenia uwag wniesionych przez Zamawiającego.
10) Produktem tego etapu prac będzie dokumentacja SZBI która musi uwzględniać wymagania wynikające z normy PN-ISO/IEC 27001 i obejmować, w szczególności poniższe obszary:
    a) polityka bezpieczeństwa informacji:
        i. polityki dotyczące bezpieczeństwa informacji,
        ii. przegląd polityk bezpieczeństwa informacji.
    b) organizacja bezpieczeństwa informacji:
        i. role i odpowiedzialność za bezpieczeństwo informacji,
        ii. rozdzielanie obowiązków,
        iii. bezpieczeństwo informacji w zarządzaniu projektami.
    c) bezpieczeństwo zasobów ludzkich:
        i. warunki zatrudnienia,
        ii. odpowiedzialność kierownicza,
        iii. uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji.
    d) zarządzanie aktywami:
        i. inwentaryzacja aktywów,
        ii. akceptowalne użycie aktywów,
        iii. zwrot aktywów,
        iv. klasyfikacja informacji,
        v. znakowanie informacji,
        vi. postępowanie z aktywami,
        vii. zarządzanie nośnikami wymiennymi,
        viii. wycofywanie nośników.
    e) przekazywanie nośników kontrola dostępu:
        i. polityka kontroli dostępu,
        ii. dostęp do sieci i usług sieciowych,
        iii. rejestrowanie i wyrejestrowywanie użytkowników,
        iv. przydzielanie dostępu użytkownikom,

Projekt „Cyfrowa gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2022. Sfinansowano w ramach reakcji Unii na pandemię COVID-19.

v. zarządzanie prawami uprzywilejowanego dostępu,
vi. zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników,
vii. przegląd praw dostępu użytkowników,
viii. odbieranie lub dostosowywanie praw dostępu,
ix. stosowanie poufnych informacji uwierzytelniających,
x. ograniczanie dostępu do informacji,
xi. procedury bezpieczeństwa logowania,
xii. system zarządzania hasłami,
xiii. użycie uprzywilejowanych programów narzędziowych.

f) kryptografia:
i. polityka stosowania zabezpieczeń kryptograficznych,
ii. zarządzanie kluczami.

g) bezpieczeństwo fizyczne i środowiskowe:
i. fizyczna granica obszaru bezpiecznego,
ii. ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
iii. praca w obszarach bezpiecznych,
iv. dostawy,
v. lokalizacja i ochrona sprzętu,
vi. bezpieczeństwo okablowania,
vii. konserwacja sprzętu,
viii. bezpieczne zbywanie lub przekazywanie do ponownego użycia,
ix. polityka czystego biurka i ekranu.

h) bezpieczna eksploatacja:
i. dokumentowanie procedur eksploatacyjnych,
ii. zarządzanie zmianą,
iii. zarządzanie pojemnością,
iv. oddzielanie środowisk rozwojowych, testowych i produkcyjnych,
v. zabezpieczenia przed szkodliwym oprogramowaniem,
vi. kopie zapasowe,
vii. rejestrowanie zdarzeń,
viii. ochrona informacji w dziennikach zdarzeń,
ix. rejestrowanie działań administratorów i operatorów,
x. synchronizacja zegarów,
xi. instalacja oprogramowania w systemach produkcyjnych,
xii. zarządzanie podatnościami technicznymi,
xiii. ograniczenia w instalowaniu oprogramowania.

i) bezpieczeństwo komunikacji:
i. zabezpieczenia sieci,
ii. polityki i procedury przesyłania informacji,
iii. porozumienia dotyczące przesyłania informacji,
iv. wiadomości elektroniczne,
v. umowy o zachowaniu poufności lub nieujawnieniu informacji,

j) pozyskiwanie, rozwój i utrzymanie systemów:

Projekt „Cyfrowa gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2022. Sfinansowano w ramach reakcji Unii na pandemię COVID-19.

i. analiza i specyfikacja wymagań związanych z bezpieczeństwem informacji,
ii. zabezpieczanie usług aplikacyjnych w sieciach publicznych,
iii. ochrona transakcji usług aplikacji,
iv. polityka bezpieczeństwa prac rozwojowych,
v. ograniczenia dotyczące zmian w pakietach oprogramowania,
vi. outsourcing,

k) relacje z dostawcami:
i. bezpieczeństwo informacji w relacji z dostawcami.

l) zarządzanie incydentami związanymi z bezpieczeństwem informacji:
i. odpowiedzialność i procedury,
ii. zgłaszanie zdarzeń związanych z bezpieczeństwem informacji,
iii. zgłaszanie słabości związanych z bezpieczeństwem informacji,
iv. ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem,
v. reagowanie na incydenty związane z bezpieczeństwem informacji,
vi. wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji,
vii. gromadzenie materiału dowodowego,

m) bezpieczeństwo informacji w zarządzaniu ciągłością działania:
i. planowanie ciągłości bezpieczeństwa informacji,
ii. wdrożenie ciągłości bezpieczeństwa informacji,

n) zgodność:
i. określenie stosowanych wymagań prawnych i umownych,
ii. ochrona zapisów,
iii. prywatność i ochrona danych identyfikujących osobę,
iv. regulacje dotyczące zabezpieczeń kryptograficznych.

9. AUDYTY WEWNĘTRZNE

W ramach usługi Wykonawca jest zobowiązany przygotować wspólnie z zespołem roboczym Zamawiającego audyty wewnętrzne Systemu Zarządzania Bezpieczeństwem Informacji, które realizowane będą w ramach procesu:

1) Inicjowanie audytu
a) wyznaczenie audytora wiodącego zespołu audytującego,
b) określenie celów, zakresu i kryteriów,
c) określenie wykonalności,
d) ustalenie zespołu audytującego,
e) ustalenie początkowego kontaktu z audytowanym.

2) Prowadzenie przeglądu dokumentacji
a) przegląd odpowiedniej dokumentacji łącznie z zapisami, określenie ich adekwatności,
b) przygotowanie działań audytowych prowadzonych u audytowanego,
c) przygotowanie planu audytu,
d) przydzielenie zadań zespołowi audytującemu,
e) przygotowanie dokumentów roboczych.

3) Prowadzenie działań audytowych u audytowanego

a) przeprowadzenie spotkania otwierającego,
b) komunikowanie się podczas audytu,
c) role i odpowiedzialności przewodników i obserwatorów,
d) zbieranie i weryfikowanie informacji,
e) opracowanie ustaleń z audytu,
f) przeprowadzenie spotkania z audytującym.

4) Przygotowanie, zatwierdzenie i dystrybucja raportu z audytu,
   a) przygotowanie raportu z audytu;
   b) zatwierdzenie i dystrybucja raportu z audytu.
5) Zakończenie audytu,
6) Zaplanowanie działań poaudytowych.

Produktem tego etapu prac będzie:
a) przeprowadzone przez Wykonawcę szkolenie dla audytorów wewnętrznych (2 x 4 godziny) potwierdzone protokołem odbioru,
b) Uzgodniony z Zamawiającym harmonogram audytów,
c) Uzgodniony z Zamawiającym Raport z audytów wewnętrznych.

10. PRZEGLĄD ZARZĄDZANIA

W ramach usługi Wykonawca jest zobowiązany przygotować i przeprowadzić wspólnie
z zespołem roboczym Zamawiającego przegląd zarządzania Systemu Zarządzania Bezpieczeństwem Informacji w ramach którego zostaną uwzględnione:
a) cele SZBI w Urzędzie;
b) obszary SZBI, które nie działają zgodnie z przeznaczeniem;
c) działania podjęte i zaplanowane w celu usunięcia wcześniej zidentyfikowanych niezgodności;
d) wyniki audytów;
e) informacje zwrotne od zainteresowanych stron;
f) wyniki oceny ryzyka i status planu postepowania z ryzykiem;
g) możliwości ciągłego doskonalenia.

Produktem tego etapu prac będzie uzgodniony z Zamawiającym Raport z przeglądu zarządzania.