Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

na przeprowadzenie audytów oraz aktualizacja, opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w ramach projektu „Cyberbezpieczny Samorząd w Gminie Izabelin”

realizowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Spis treści

Izabelin, luty 2025 r.

1 Zakres zamówienia

Przedmiotem zamówienia jest przeprowadzenie audytów oraz aktualizacja, opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w ramach projektu „Cyberbezpieczny Samorząd w Gminie Izabelin" współfinansowanego z *Funduszy Europejskich na Rozwój Cyfrowy (FERC) II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusz Europejski Fundusz Rozwoju Regionalnego (EFRR), Numer naboru FERC.02.02-CS.01-001/23*

1. **ETAP I:** przeprowadzenie audytu przedwdrożeniowego bezpieczeństwa informacji wraz z testami bezpieczeństwa.
2. **ETAP II:** Aktualizacja, opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz Audytu KRI.
3. **ETAP III:** przeprowadzenie Audytu Cyberbezpieczeństwa końcowego wraz z testami bezpieczeństwa oraz sporządzenie „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego", o których mowa w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd", opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem http://www.gov.pl/cppc/cyberbezpieczny-samorzad.

Informacje dotyczące Jednostek objętych przedmiotem zamówienia

Jednostki objęte przedmiotem zamówienia:

a. Urząd Gminy Izabelin – ul. 3 Maja 42, 05-080 Izabelin C;
b. Gminny Ośrodek Pomocy Społecznej w Izabelinie - 3 Maja 42, 05-080 Izabelin C;
c. Centrum Usług Wspólnych w Izabelinie - ul. Szkolna 2A, Hornówek, 05-080 Izabelin.

Dane/informacje dot. inrastruktury	Urząd Gminy Izabelin	Gminny Ośrodek Pomocy Społecznej w Izabelinie	Centrum Usług Wspólnych w Izabelinie
Ilość pracowników/ użytkowników w Urzędzie i JP	72 Pracowników 72 Użytkowników	23 Pracowników 18 Użytkowników	17 Pracowników 13 Użytkowników
Ilość komputerów (również przenośnych)	79 szt.	28 szt.	12 szt.
Ilość serwerów (fizycznych, wirtualnych)	4 Fizycznych 18 wirtualnych	0 Fizycznych 0 wirtualnych	1 Fizycznych 0 wirtualnych
Ilość pozostałych urządzeń Podłączonych do sieci	Łącznie 33 w tym switch – ok.15 łącznie z GOPS UTM – 1 Macierz – 1 QNAP i Synology - 2 NAS - 1 Drukarki sieciowe – ok.13	Łącznie 5 w tym switch - UTM - Macierz - NAS - 1 Drukarki sieciowe - 4	Łącznie 2 w tym switch - 1 UTM - Macierz - NAS – QNAP – 1 Drukarki sieciowe – nie wiem
Ilość serwerowni	1	0	0

Czy wdrożono AD	Tak	Tak	Tak

Audyt bezpieczeństwa ma zostać przeprowadzony w oparciu o Standardy: Krajowe Ramy Interoperacyjności (KRI), Krajowy System Cyberbezpieczeństwa (KSC), normę ISO27001:2023 oraz Narodowe Standardy Cyberbezpieczeństwa (NSC).

Testy penetracyjne (bezpieczeństwa) mają zostać przeprowadzone zgodnie z Metodologią PTES Standard.

Wykonanie i przekazanie Raportu z Audytu zawierającego w szczególności: opis zakresu przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytów, wnioski i zalecenia związane z rozwiązaniem występujących problemów, analiza złożonego załącznika nr 6 do konkursu grantowego tj. „Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)".

Istotą testów jest bezstronne zapewnienie, że infrastruktura spełnia standardy bezpieczeństwa w obszarze Eksploatacji systemów - zapewnienie ciągłości działania systemów informatycznych z uwzględnieniem aspektów poufności, rozliczalności, dostępności oraz integralności przetwarzanych informacji.

Przygotowanie do audytu:

a) Zebranie wstępnych informacji za pomocą pisemnych i telefonicznych konsultacji z przedstawicielem Zamawiającego, w zależności od złożoności przeprowadzanego audytu i testów.

b) Kompletacja danych istotnych dla audytu i testów.

c) Określenie rodzaju audytu – White Box. W przypadku audytu na znanej infrastrukturze, niezbędne jest dostarczenie dokumentacji umożliwiającej określenie topologii sieci.

d) Przeprowadzenie wywiadu technicznego z osobą posiadającą szczegółową wiedzę na temat urządzeń i usług mających wpływ na bezpieczeństwo organizacji.

e) Upewnienie się, że obecna jest osoba uprawniona do zagwarantowania fizycznego dostępu do elementów infrastruktury sieciowej (szczególnie serwerowni, urządzeń brzegowych, przełączników sieciowych, węzłów komunikacyjnych, punktów dostępowych).

f) Przedstawienie przedstawicielowi organizacji zakresu audytu lub testów penetracyjnych wraz ze szczegółowym określeniem zasad, warunków i zakresu przeprowadzanych działań.

Wymagania proceduralne

Audyt zostanie przeprowadzony zgodnie z wymogami dokumentacji konkursowej oraz najlepszymi, obowiązującymi praktykami. Wykonanie testów bezpieczeństwa zostanie zlecone niezależnemu wykonawcy, który nie jest powiązany z żadnym elementem (w tym producentem urządzeń) testowanej infrastruktury oraz organizacji, co gwarantuje obiektywność i rzetelność przeprowadzonej analizy.

2 Termin realizacji

ETAP I – 45 dni kalendarzowych od dnia zawarcia umowy;

ETAP II – 120 dni kalendarzowych od dnia zakończenia etapu I;

ETAP III – 60 dni po otrzymaniu informacji od Zamawiającego drogą e-mailową o gotowości do poddania się badaniu audytowemu, a przed złożeniem przez Zamawiającego wniosku rozliczającego otrzymany grant.

3 Szczegółowy opis zakresu

1.1 ETAP I

Przeprowadzenie audytu przedwdrożeniowego bezpieczeństwa informacji wraz z testami bezpieczeństwa w celu oceny zgodności systemów teleinformatycznych z normami i politykami bezpieczeństwa.

Przeprowadzenie audytu w oparciu o wymagania Polskiej Normy PN-EN ISO/1EC 27 001 oraz zgodnego z wytycznymi PN-EN ISO 19011:2019. Audyt umożliwi identyfikację i ocenę ryzyka informatycznego u Zamawiającego, a także udoskonalanie procedur zarządzania w organizacji wg wskazanych norm oraz, wytycznych z określonych rozporządzeń, dyrektyw (w tym NIS2), ustaw (w tym Ustawa o Krajowym Systemie Cyberhezpieczeństwa - dalej zwana ustawą KSC). Zamawiający zabezpiecza się w ten sposób m.in. przed niebezpieczeństwami związanymi z integralnością, poufnością, wydajnością czy niezawodnością infrastruktury.

Efektem audytu będzie poprawa procedur dotyczących dostępu do danych oraz zachowanie ich poufności. W ten sposób zmniejsza się ryzyko sytuacji wejścia przez nieuprawnione osoby w posiadanie wrażliwych informacji.

Audyt zostanie przeprowadzony w jednostkach:

a. Urząd Gminy Izabelin;
b. Gminny Ośrodek Pomocy Społecznej w Izabelinie;
c. Centrum Usług Wspólnych w Izabelinie.

Zakres działań na rzecz realizacji zadania:

1. Audyt organizacyjny:
   a) weryfikacja regulacji w obszarze zarządzania bezpieczeństwem informacji;
   b) odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;
   c) dokumentacja, w tym z zakresu ochrony danych osobowych;
   d) analiza ryzyka;
   e) inwentaryzacja aktywów;
   f) plan postępowania z ryzykiem;
   g) przeprowadzenie wywiadów z wybranymi pracownikami.
2. Audyt fizyczny i środowiskowy

a) weryfikacja zabezpieczeń wejścia/wyjścia;

b) weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń;

c) weryfikacja bezpieczeństwa okablowania strukturalnego;

d) weryfikacja systemów chłodzenia i systemów alarmowych.

3. Audyt teleinformatyczny (testy bezpieczeństwa)

Audyt teleinformatyczny (testy bezpieczeństwa) dotyczyć muszą:

a) Usług oraz zasobów publicznie dostępnych w sieci Internet:

- Ocena podatności na ataki: Wykonanie skanowania pod względem podatności i oceny zgodności z najlepszymi praktykami zabezpieczeń.
- Urządzenia brzegowe: Sprawdzenie konfiguracji firewalli, IPS/IDS, mechanizmów anty DDoS oraz zabezpieczeń SSL/TLS.

b) Bezpieczeństwa poczty elektronicznej

- Weryfikacja poprawności konfiguracji mechanizmów SPF, DMARC, DKIM.
- Szyfrowanie poczty: Ocena implementacji szyfrowania (S/MIME, PGP), bezpieczne przechowywanie i zarządzanie kluczami.

c) Bezpieczeństwa infrastruktury sieciowej

- Konfiguracja urządzeń sieciowych: Szczegółowa analiza konfiguracji firewalli, routerów, przełączników oraz punktów dostępowych, ocena segmentacji sieci i VLAN.
- Analiza bezpieczeństwa sieci wewnętrznych i zewnętrznych, ocena bezpieczeństwa VPN.
- Analiza udostępnionych usług wraz z testami bezpieczeństwa mającymi na celu weryfikację istnienia podatności na ataki sieciowe.

d) Bezpieczeństwa infrastruktury sprzętowej i oprogramowania

- weryfikacja aktualizacji systemów operacyjnych, aplikacji, firmware urządzeń.
- ocena weryfikacja wdrożonych polityk bezpieczeństwa oraz zarządzania zasobami IT pod względem stosowania bezpiecznych praktyk administracyjnych.

e) Bezpiecznej konfiguracja domeny Microsoft Active Directory

- weryfikacja poprawnej konfiguracji domeny oraz wdrożonych polityk bezpieczeństwa wraz z oceną zabezpieczeń Kerberos I analizą polityki haseł.
- weryfikacja GPO (Group Policy Objects), audyt uprawnień użytkowników i grup, analiza logowania i monitorowania zdarzeń.

f) Bezpieczeństwa aplikacji

- Aplikacje utrzymywane w sieci wewnętrznej zostaną poddane analizie, której celem jest określenie stopnia podatności na ataki.
- W zależności od rodzaju aplikacji występujących w środowisku klienta, zastosowane zostaną dopasowane techniki pozwalające na wykrycie luk oraz błędów w obszarach związanych z

daną usługą, w tym zostanie przeprowadzona weryfikacja konfiguracji baz danych, ocena mechanizmów autoryzacji i uwierzytelnienia pod względem podatności na ataki.

g) Bezpieczeństwa danych – backupy

- Ocena polityki backupów w organizacji, w tym częstotliwości tworzenia kopii zapasowych i ich przechowywania.
- Weryfikacja zgodności procedur backupowych z przyjętymi standardami branżowymi.
- Sprawdzenie, czy kopie zapasowe przechowywane są w odseparowanych, bezpiecznych i oddzielnych lokalizacjach.
- Weryfikacja szyfrowania kopii zapasowych w celu ochrony przed nieautoryzowanym dostępem.

h) Poprawności aktualnej dokumentacji

- Sprawdzenie, czy dokumentacja dotycząca bezpieczeństwa jest kompletna i zgodna z obowiązującymi standardami.

i) Testów socjotechnicznych

- Przeprowadzenie symulowanych ataków phishingowych, ocena wyników i opracowanie rekomendacji na podstawie zachowań pracowników.
- Kampania zostanie podzielona na trzy grupy odbiorców, aby ocenić różne poziomy wrażliwości i odpowiedzi na tego typu zagrożenia.
- Szczegółowe wymagania do przeprowadzenia testów socjotechnicznych:
  - Wykonawca będzie zobowiązany do zachowania poufności i przestrzegania przepisów o ochronie danych osobowych oraz do prowadzenia audytu w sposób uczciwy i obiektywny.
  - Przygotowanie co najmniej 3 zdefiniowanych scenariuszy ataków, na podstawie przekazanych przez Zamawiającego informacji (podejrzane wiadomości e-mail).
  - Dostosowanie przygotowanych scenariuszy do specyfiki Zamawiającego (wspólne uzgodnienie z Zamawiającym).
  - Przeprowadzenie co najmniej 6 ataków socjotechnicznych mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie ludzkiego czynnika jako wektora ataku.
  - W przypadku skuteczności ataku analizę danych i informacji w skrzynkach pocztowych takich pracowników celem określenia ich przydatności do dalszej eskalacji ataku.
  - Przygotowanie raportu z przeprowadzonych ataków z odniesieniem do opisu scenariuszy ataków, oceny skuteczności ataków, Informacji o zaatakowanych pracownikach i wrażliwych danych, rekomendacje dotyczące poprawy bezpieczeństwa.
  - Zamawiający zapewni dodanie serwerów wysyłkowych Wykonawcy do list wykluczeń filtrów antyspamowych i antyphishingowych.

- Wykonawca zapewni, że „złośliwe" załączniki zawierać będą jedynie prosty program odsyłający na serwer Wykonawcy dane telemetryczne na temat zaatakowanej maszyny bez przejęcia nad nią „całkowitej" kontroli.
- Zamawiający wyraża zgodę na wykorzystanie wizerunku Zamawiającego w tym w szczególności: logo, nazwy domeny i grafiki, stopki podpisu wiadomości e-mail w czasie trwania testów bezpieczeństwa w postaci testów socjotechnicznych.

1.2 ETAP II

Aktualizacja, opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz Audytu KRI w jednostkach:

a. Urząd Gminy Izabelin,

b. Gminny Ośrodek Pomocy Społecznej w Izabelinie

c. Centrum Usług Wspólnych w Izabelinie

1.2.1 System Zarządzania Bezpieczeństwem Informacji

Zamawiający jest świadomy, że dla prawidłowego wdrożenia i funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji na wszystkich etapach już od rozpoczęcia opracowywania niezbędne jest zaangażowanie, wsparcie i współdziałanie ze strony wszystkich pracowników organizacji. Poniżej wymienione pozycje w procesie budowania SZBI nie muszą stanowić katalogu zamkniętego i będą dostosowane do indywidualnych potrzeb organizacji oraz zgodnie z obowiązującymi przepisami prawa.

Zakres działań na rzecz realizacji zadania:

a) Ocena bieżących praktyk w obszarze bezpieczeństwa informacji oraz analiza istniejącej dokumentacji z obszaru bezpieczeństwa informacji i ochrony danych osobowych, stosowanych zabezpieczeń technicznych i organizacyjnych.

b) Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):

- W oparciu o przeprowadzona wcześniej analizę dokonanie aktualizacji lub doskonalenie istniejącej dokumentacji a w przypadku braku opracowanie polityki bezpieczeństwa informacji zgodnej z wymaganiami normy ISO/IEC 27001.
- Określenie celów i wskaźników na potrzeby monitorowania, pomiarów, analizy i oceny systemu zarządzania.
- Opracowanie polityk tematycznych, procedur, wytycznych i dokumentacji operacyjnej (adekwatnie do potrzeb organizacji), w poszczególnych obszarach jak np.:
  - Zarządzania Tożsamością i Dostępem obejmujących w szczególności:
    - zasady przydzielania i odwoływania uprawnień dostępu do systemów i danych;
    - procedura rejestracji użytkowników i zarządzania ich kontami;
    - zarządzanie personelem i bezpieczeństwo zasobów ludzkich;
    - monitorowanie i audyt działań użytkowników;

- zarządzania autoryzacją użytkowników w SI;
- zarządzanie w obszarze świadomości personelu - szkolenia i świadomość bezpieczeństwa:
  - planowanie i realizacja szkoleń w zakresie bezpieczeństwa informacji dla pracowników;
  - monitorowanie świadomości pracowników na temat zagrożeń i praktyk bezpieczeństwa;
  - uświadamianie pracowników w zakresie cyberbezpieczeństwa.

- Kontekst organizacji – identyfikacja wymagań i monitorowanie zmian;
- Zarządzanie bezpieczeństwem fizycznym;
- Zarządzanie bezpieczeństwem osobowym;
- Zarządzanie bezpieczeństwem środowiskowym;
- Zarządzanie bezpieczeństwem sprzętu;
- Zarządzanie bezpieczeństwem nośników danych;
- Zarządzania tożsamością (prawami dostępu);
- Zarządzanie bezpieczeństwem sieci;
- Zarządzanie bezpieczeństwem komunikacji;
- Stosowanie zabezpieczeń kryptograficznych;
- Zarządzanie Zagrożeniami i Podatnościami;
- Zarządzania Incydentami Bezpieczeństwa i Zdarzeniami Bezpieczeństwa:
  - Procedura zgłaszania, monitorowania i reagowania na zaistniałe incydenty bezpieczeństwa;
  - Procedura działania doskonalące;
  - Monitorowanie i analiza zdarzeń związanych z bezpieczeństwem informacji.
  - Zarządzanie działaniami korygującymi i zapobiegawczymi - procedura identyfikacji, dokumentacji i realizacji działań korygujących w wyniku incydentów i nieprawidłowości w celu zapobiegania przyszłym incydentom.
  - Zarządzanie zgodnością z wymaganiami prawnymi, umownymi oraz wewnętrznymi regulacjami.
  - Procedura inwentaryzacji aktywów i postępowania z ryzykiem.
  - Plan doskonalenia i postepowania z ryzykiem.
  - Procedura postępowania z incydentami związanymi z ochroną danych osobowych i bezpieczeństwem informacji.
- Zarządzania Ryzykiem:
  - Ocena ryzyka związanego z informacjami i danymi.

- Określenie strategii i zarządzania ryzykiem.
- Monitorowanie i aktualizacja oceny ryzyka, postępowanie z ryzykiem.

- Bezpieczeństwo relacji z Dostawcami:
  - Ocena i wybór dostawców z uwzględnieniem bezpieczeństwa informacji.
  - Monitorowanie dostawców pod kątem przestrzegania standardów bezpieczeństwa.
- Zarządzanie monitorowaniem i audytem:
  - Monitorowanie systemów i sieci w celu wykrywania nieprawidłowości i potencjalnych zagrożeń.
  - Przeprowadzanie audytów bezpieczeństwa – planowanie, realizowanie, dokumentowanie.
  - Procedura audyt wewnętrzny.
- Zarządzanie dokumentacją i zapisami, zarządzanie Politykami i Procedurami SZBI:
  - Tworzenie, kontrolowanie, przeglądy, aktualizacja i zarządzanie dokumentacją związaną z bezpieczeństwem informacji.
  - Przechowywanie, znakowanie i udostępnianie dokumentacji.
  - Tworzenie, aktualizacja i komunikacja polityk bezpieczeństwa informacji oraz procedur wewnętrznych.
  - Procedura przegląd systemu zarządzania ochroną danych osobowych i bezpieczeństwem informacji.
  - Procedura nadzór nad dokumentami.
- Zarządzania Ciągłością Działania:
  - Planowanie i wdrażanie środków zapewniających ciągłość działania w przypadku awarii lub incydentów.
  - Procedura zarzadzanie ciągłością działania.
- Przeglądy zarządzania ISMS:
  - Zarządzanie cyberbezpieczeństwem w relacjach z dostawcami i wykonawcami.
  - Zarządzania cyberbezpieczeństwem w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych.
  - Przegląd Audytów cyberbezpieczeństwa.

- Opracowanie Deklaracji stosowania zabezpieczeń wg wymagań Załącznika A normy PN-EN ISO/IEC 27001:2023
- Wdrożenie SZBI – działania związane z wdrożeniem do stosowania uzgodnionych procedur i zasad postępowania, konsultacje i instruktarz w zakresie dokumentowania działań, tworzenia zapisów SZBI, konsultacje i instruktaż dla osób pełniących kluczowe role w ramach SZBI.

1.2.2 AUDYT KRI

Audyt KRI musi obejmować Analizę czy wymagania określone w ***Rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*** zostały spełnione.

Zakres działań prowadzonych w ramach audytu KRI polegać będzie na weryfikacji, czy organizacja spełnia wymagania określone w Rozporządzeniu jako:

1) zamieszczenie na głównej stronie internetowej podmiotu (i/lub na stronie BIP), odesłania do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług, terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw, zgodnie z § 5 ust. 2 pkt 1 i 4;
2) Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk zgodnie z § 15. ust. 1.
3) Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury zgodnie z § 15. ust.2;
4) Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących, zgodnie z §16. ust.1.
5) sposób udostępniania zasobów informatycznych z systemów teleinformatycznych, zgodnie z §18 ust. 1 Rozporządzenia KRI;
6) sposób przyjmowania dokumentów elektronicznych przez systemy teleinformatyczne, zgodnie z §18 ust. 2 Rozporządzenia KRI;
7) opracowanie, ustanowienie, wdrożenie i eksploatacja, monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z §19 ust. 1;
8) aktualizacja regulacji wewnętrznych zgodnie z §19 ust. 2 pkt.1) ;
9) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację z §19 ust. 2 pkt.2);
10) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji zgodnie z §19 ust. 2 pkt.3);
11) zapewnienie adekwatności poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji, zgodnie z §19 ust. 2 pkt 4);
12) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, zgodnie z §19 ust. 2 pkt.5);

13) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji, zgodnie z §19 ust. 2 pkt.6);

14) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

a) monitorowanie dostępu do informacji,

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji; zgodnie z §19 ust. 2 pkt.7);

15) ustanowienie zasad telepracy oraz pracę przy przetwarzaniu mobilnym zgodnie z§19 ust. 2 pkt.8);

16) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie zgodnie z§19 ust. 2 pkt.9);

17) zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji zgodnie z§19 ust. 2 pkt.10);

18) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych zgodnie z §19 ust. 2 pkt.11);

19) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa

zgodnie z §19 ust.12 pkt a)-h);

20) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących zgodnie z §19 ust.13);

21) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. zgodnie z §19 ust.14).

1.3 ETAP III

Przeprowadzenie audytu powdrożeniowego systemu zarządzania bezpieczeństwem informacji wraz z testami bezpieczeństwa oraz sporządzenie „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego", o których mowa w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd" opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem http://www.gov.pl/cppc/cyberbezpieczny-samorzad.

Audyt ma na celu:

- ocenę skuteczności wdrożenia SZBI;
- weryfikacja zgodności z normami PN-EN ISO/IEC 27001:2023, PN-EN ISO/IEC 27002 i PN-ISO/IEC 27005.

Przeprowadzenie audytu w oparciu o wymagania Polskiej Normy PN-EN ISO/1EC 27 001 oraz zgodnego z wytycznymi PN-EN ISO 19011:2019. Audyt umożliwi identyfikację i ocenę ryzyka informatycznego u Zamawiającego, a także udoskonalanie procedur zarządzania w organizacji wg wskazanych norm oraz, wytycznych z określonych rozporządzeń, dyrektyw (w tym NIS2), ustaw (w tym Ustawa o Krajowym Systemie Cyberhezpieczeństwa - dalej zwana ustawą KSC). Zamawiający zabezpiecza się w ten sposób m.in. przed niebezpieczeństwami związanymi z integralnością, poufnością, wydajnością czy niezawodnością infrastruktury.

Ankieta i audyt zostaną przeprowadzone w Jednostkach:

a. Urząd Gminy Izabelin,
b. Gminny Ośrodek Pomocy Społecznej w Izabelinie
c. Centrum Usług Wspólnych w Izabelinie.

Zakres działań na rzecz realizacji zadania:

1. Audyt organizacyjny:
   a) weryfikacja regulacji w obszarze zarządzania bezpieczeństwem informacji;
   b) odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;
   c) dokumentacja, w tym z zakresu ochrony danych osobowych;
   d) analiza ryzyka;
   e) inwentaryzacja aktywów;
   f) plan postępowania z ryzykiem;
   g) przeprowadzenie wywiadów z wybranymi pracownikami.
2. Audyt fizyczny i środowiskowy
   a) weryfikacja zabezpieczeń wejścia/wyjścia;

b) weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń;

c) weryfikacja bezpieczeństwa okablowania strukturalnego;

d) weryfikacja systemów chłodzenia i systemów alarmowych.

3. Audyt teleinformatyczny (testy bezpieczeństwa)

Audyt teleinformatyczny (testy bezpieczeństwa) dotyczyć muszą:

a) Usług oraz zasobów publicznie dostępnych w sieci Internet:

- Ocena podatności na ataki: Wykonanie skanowania pod względem podatności i oceny zgodności z najlepszymi praktykami zabezpieczeń.
- Urządzenia brzegowe: Sprawdzenie konfiguracji firewalli, IPS/IDS, mechanizmów anty DDoS oraz zabezpieczeń SSL/TLS.

b) Bezpieczeństwa poczty elektronicznej

- Weryfikacja poprawności konfiguracji mechanizmów SPF, DMARC, DKIM.
- Szyfrowanie poczty: Ocena implementacji szyfrowania (S/MIME, PGP), bezpieczne przechowywanie i zarządzanie kluczami.

c) Bezpieczeństwa infrastruktury sieciowej

- Konfiguracja urządzeń sieciowych: Szczegółowa analiza konfiguracji firewalli, routerów, przełączników oraz punktów dostępowych, ocena segmentacji sieci i VLAN.
- Analiza bezpieczeństwa sieci wewnętrznych i zewnętrznych, ocena bezpieczeństwa VPN.
- Analiza udostępnionych usług wraz z testami bezpieczeństwa mającymi na celu weryfikację istnienia podatności na ataki sieciowe.

d) Bezpieczeństwa infrastruktury sprzętowej i oprogramowania

- weryfikacja aktualizacji systemów operacyjnych, aplikacji, firmware urządzeń.
- ocena weryfikacja wdrożonych polityk bezpieczeństwa oraz zarządzania zasobami IT pod względem stosowania bezpiecznych praktyk administracyjnych.

e) Bezpiecznej konfiguracja domeny Microsoft Active Directory

- weryfikacja poprawnej konfiguracji domeny oraz wdrożonych polityk bezpieczeństwa wraz z oceną zabezpieczeń Kerberos I analizą polityki haseł.
- weryfikacja GPO (Group Policy Objects), audyt uprawnień użytkowników i grup, analiza logowania i monitorowania zdarzeń.

f) Bezpieczeństwa aplikacji

- Aplikacje utrzymywane w sieci wewnętrznej zostaną poddane analizie, której celem jest określenie stopnia podatności na ataki.
- W zależności od rodzaju aplikacji występujących w środowisku klienta, zastosowane zostaną dopasowane techniki pozwalające na wykrycie luk oraz błędów w obszarach związanych z daną usługą, w tym zostanie przeprowadzona weryfikacja konfiguracji baz danych, ocena mechanizmów autoryzacji i uwierzytelnienia pod względem podatności na ataki.

g) Bezpieczeństwa danych – backupy

- Ocena polityki backupów w organizacji, w tym częstotliwości tworzenia kopii zapasowych i ich przechowywania.
- Weryfikacja zgodności procedur backupowych z przyjętymi standardami branżowymi.
- Sprawdzenie, czy kopie zapasowe przechowywane są w odseparowanych, bezpiecznych i oddzielnych lokalizacjach.
- Weryfikacja szyfrowania kopii zapasowych w celu ochrony przed nieautoryzowanym dostępem.

h) Poprawności aktualnej dokumentacji

- Sprawdzenie, czy dokumentacja dotycząca bezpieczeństwa jest kompletna i zgodna z obowiązującymi standardami.

i) Testów socjotechnicznych

- Przeprowadzenie symulowanych ataków phishingowych, ocena wyników i opracowanie rekomendacji na podstawie zachowań pracowników.
- Kampania zostanie podzielona na trzy grupy odbiorców, aby ocenić różne poziomy wrażliwości i odpowiedzi na tego typu zagrożenia.
- Szczegółowe wymagania do przeprowadzenia testów socjotechnicznych:
  - Wykonawca będzie zobowiązany do zachowania poufności i przestrzegania przepisów o ochronie danych osobowych oraz do prowadzenia audytu w sposób uczciwy i obiektywny.
  - Przygotowanie co najmniej 3 zdefiniowanych scenariuszy ataków, na podstawie przekazanych przez Zamawiającego informacji (podejrzane wiadomości e-mail).
  - Dostosowanie przygotowanych scenariuszy do specyfiki Zamawiającego (wspólne uzgodnienie z Zamawiającym).
  - Przeprowadzenie co najmniej 6 ataków socjotechnicznych mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie ludzkiego czynnika jako wektora ataku.
  - W przypadku skuteczności ataku analizę danych i informacji w skrzynkach pocztowych takich pracowników celem określenia ich przydatności do dalszej eskalacji ataku.
  - Przygotowanie raportu z przeprowadzonych ataków z odniesieniem do opisu scenariuszy ataków, oceny skuteczności ataków, Informacji o zaatakowanych pracownikach i wrażliwych danych, rekomendacje dotyczące poprawy bezpieczeństwa.
  - Zamawiający zapewni dodanie serwerów wysyłkowych Wykonawcy do list wykluczeń filtrów antyspamowych i antyphishingowych.
  - Wykonawca zapewni, że „złośliwe” załączniki zawierać będą jedynie prosty program odsyłający na serwer Wykonawcy dane telemetryczne na temat zaatakowanej maszyny bez przejęcia nad nią „całkowitej” kontroli.

- Zamawiający wyraża zgodę na wykorzystanie wizerunku Zamawiającego w tym w szczególności: logo, nazwy domeny i grafiki, stopki podpisu wiadomości e-mail w czasie trwania testów bezpieczeństwa w postaci testów socjotechnicznych.

Wykonawca ma obowiązek sporządzić „Ankietę Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego", o których mowa w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd" opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem http://www.gov.pl/cppc/cyberbezpieczny-samorzad dla: Urzędu Gminy Izabelin, Gminnego Ośrodka Pomocy Społecznej w Izabelinie oraz Centrum Usług Wspólnych w Izabelinie.

4 Przygotowanie raportu z Audytu

Wynikiem przeprowadzonych Audytów mają być pisemne raporty, określające poziom spełnienia wymagań tj. podsumowanie, przedstawienie wyników, procesów naprawczych w celu poprawy bezpieczeństwa organizacji:

a. Przygotowanie raportu zawierającego szczegółowe wyniki wizji lokalnej.

b. Wyróżnienie obszarów wymagających uwagi oraz silnych stron zabezpieczeń fizycznych.

c. Lista konkretnych podatności z ich nazwami, numerami CVE (Common Vulnerabilities and Exposures), szczegółowymi opisami, oraz rekomendacjami ich usunięcia lub zminimalizowania skutków zidentyfikowanej podatności.

d. Załączenie zrzutów ekranu, logów oraz innych danych wspierających identyfikację podatności.

e. Wskazanie liczby podatności sklasyfikowanych jako niskie, średnie, wysokie i krytyczne.

f. Opis potencjalnych skutków wykorzystania każdej podatności (np. utrata danych, przerwy w dostępności, ataki hakerskie).

g. Wskazanie, które podatności powinny być naprawione jako pierwsze, bazując na ich krytyczności i potencjalnych skutkach.

h. Informacje na temat warunków, w jakich skanowanie zostało przeprowadzone.

Zamawiający nie dopuszcza kopiowania treści ogólnodostępnych w formie nieprzetworzonej (dostępnych w Internecie). Dokumenty będą zawierać przywołania zamiast cytowania tekstów analizowanych i powszechnie dostępnych. Dokumentacja ma zawierać wyłącznie autorskie treści, powstałe w wyniku realizacji zamówienia oraz inne autorskie treści wykonawcy, które nie są publicznie dostępne. Będą opracowaniem kompletnym, wyczerpującym i dostosowanym do potrzeb organizacji, z punktu widzenia celu, któremu mają służyć.

Wykonawca zobowiązany jest do przeniesienia na Zamawiającego autorskich praw majątkowych do całości przedmiotu wykonanego w ramach przedmiotu zamówienia, w szczególności do wszelkich opracowanych przez Wykonawcę dokumentów oraz ich wersji roboczych, w ramach wynagrodzenia umownego z chwilą przekazania ich Zamawiającemu, zgodnie z przepisami ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2022 poz. 2509 z późn. zm.).