Załącznik nr 2 – Opis przedmiotu zamówienia

Zamawiający:
Gmina Mirów, Mirów Stary 27, 26-503 Mirów

OPIS PRZEDMIOTU ZAMÓWIENIA

1/ przeprowadzenie audytu systemu zarządzania bezpieczeństwem informacji wraz z wypełnieniem końcowej ankiety dojrzałości do projektu Cyberbezpieczny Samorząd

Zamawiający informuje, że celem audytu jest kompleksowa ocena skuteczności funkcjonowania systemu zarządzania bezpieczeństwem informacji (SZBI) ora spełnienia minimalnych wymagań Rozporządzenia KRI oraz zgodności z przepisami prawa powszechnie obowiązującego.

Zamawiający wymaga, aby zakres audytu obejmował następujące obszary:

1. Zarządzanie SZBI:

- weryfikacja poprawności ustanowienia, wdrożenia, utrzymania, monitorowania i doskonalenia SZBI,
- ocena zaangażowania najwyższego kierownictwa, w tym zapewnienia zasobów, nadzoru nad realizacją polityk bezpieczeństwa oraz przypisania ról i odpowiedzialności w obszarze SZBI,
- ocena skuteczności nadzoru nad aktualizacją regulacji wewnętrznych w odpowiedzi na zmieniające się otoczenie prawne, organizacyjne i technologiczne,
- weryfikacja realizacji szkoleń i działań podnoszących świadomość pracowników w zakresie ochrony informacji.

2. Zarządzanie ryzykiem:

- analiza kompletności i aktualności inwentaryzacji aktywów (sprzętu, oprogramowania, informacji),
- ocena skuteczności przeprowadzanych analiz ryzyka utraty poufności, integralności i dostępności informacji,
- weryfikacja wdrożonych planów postępowania z ryzykiem oraz podejmowania działań adekwatnych do poziomu ryzyka,
- nadzór nad przeglądem i aktualizacją rejestru ryzyk oraz dokumentacją potwierdzającą proces zarządzania ryzykiem.

3. Bezpieczeństwo techniczne i fizyczne:

- weryfikacja skuteczności zabezpieczeń systemów informatycznych, w tym ochrony przed błędami, nieautoryzowaną modyfikacją, zniszczeniem lub utratą danych,
- kontrola zgodności systemów teleinformatycznych z politykami bezpieczeństwa,
- weryfikacja stosowania mechanizmów kryptograficznych w celu ochrony poufności i integralności informacji,
- analiza procesów zarządzania podatnościami, w tym reagowania na opublikowane i nowo wykryte luki bezpieczeństwa,
- ocena bezpieczeństwa fizycznego pomieszczeń oraz urządzeń przetwarzających informacje, a także zabezpieczeń wejścia/wyjścia.

4. Zarządzanie dostępem i uprawnieniami:

- ocena procesu nadawania, modyfikowania, zawieszania i odbierania uprawnień użytkowników,
- weryfikacja skuteczności kontroli dostępu logicznego do systemów i informacji,
- analiza mechanizmów monitorowania aktywności użytkowników oraz wykrywania naruszeń.

5. Praca zdalna:

- weryfikacja polityk i procedur dotyczących bezpiecznej pracy zdalnej,
- ocena stosowanych zabezpieczeń technicznych oraz nadzoru nad przestrzeganiem zasad pracy poza siedzibą organizacji.

6. Współpraca z podmiotami trzecimi:

- analiza umów i porozumień z dostawcami zewnętrznymi w kontekście zapewnienia bezpieczeństwa informacji,
- weryfikacja obowiązków w zakresie ochrony danych osobowych oraz odpowiedzialności za incydenty bezpieczeństwa.

7. Dokumentacja i zgodność z przepisami:

- weryfikacja kompletności i aktualności dokumentacji SZBI, w tym procedur, polityk, rejestrów i planów ciągłości działania,
- ocena procesów przeglądu i aktualizacji dokumentacji SZBI.

Audyt powinien zakończyć się sporządzeniem raportu zawierającego opis stanu faktycznego, identyfikację niezgodności i luk, ocenę zgodności z wymaganiami oraz zalecenia naprawcze i działania doskonalące.

Zamawiający zezwala, aby Wykonawca przeprowadził możliwe do realizacji czynności wynikające z przedmiotu zamówienia w formule online.

2/ przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy Mirów

Zamawiający wymaga jednokrotnego przeprowadzenia szkolenia dla pracowników Urzędu Gminy Mirów. Ilość pracowników: 21 osób. Zamawiający wymaga, aby szkolenie przeprowadzone zostało z podziałem na dwie grupy szkoleniowe, po 2 h szkolenia dla każdej z grup. Szkolenie dla obu grup powinno odbyć się w formie online i zostać zorganizowane w trakcie jednego dnia roboczego.

Tematyka szkolenia powinna zawierać minimum omówienie poprawnych zasad związanych z cyberbezpieczeństwem. Ponadto wymaga się, aby zostały omówione zagrożenia w sieci takie jak phishing, ransomware oraz malware, które powodują poważne zagrożenia dla bezpieczeństwa informacji.

Zamawiający określa minimalny zakres szkolenia:

1. Wprowadzenie do cyberbezpieczeństwa - definicja i znaczenie cyberbezpieczeństwa w administracji publicznej. Omówienie roli i odpowiedzialności pracowników w utrzymaniu bezpieczeństwa informacji.
2. Podstawowe zasady cyberbezpieczeństwa - omówienie fundamentalnych reguł i procedur dotyczących ochrony danych, zarządzania hasłami, autoryzacji i bezpiecznego korzystania z zasobów informatycznych.
3. Phishing i inne ataki socjotechniczne - rozpoznawanie i ochrona przed próbami wyłudzenia informacji, atakami phishingowymi oraz innymi technikami socjotechnicznymi.
4. Zagrożenia związane z oprogramowaniem typu ransomware i malware - identyfikacja, mechanizmy działania oraz metody zapobiegania i reagowania na zagrożenia związane z ransomware i malware.
5. Bezpieczna obsługa poczty elektronicznej - zasady korzystania z e-maila, rozpoznawanie podejrzanych wiadomości, załączników oraz linków, a także ochrona przed spamem i phishingiem.
6. Zarządzanie hasłami i autoryzacja - tworzenie silnych haseł, korzystanie z menedżerów haseł, wprowadzenie autoryzacji dwuetapowej oraz znaczenie kluczy sprzętowych.
7. Ochrona urządzeń mobilnych - zabezpieczanie urządzeń przenośnych, takich jak smartfony
   i tablety, przed utratą danych, kradzieżą oraz złośliwym oprogramowaniem.
8. Bezpieczne przetwarzanie i przechowywanie danych - szyfrowanie danych, zasady bezpiecznego przechowywania informacji, zarządzanie dostępem oraz udostępnianie danych w sposób bezpieczny.

9. **Zarządzanie ryzykiem w cyberbezpieczeństwie** - identyfikacja i ocena ryzyka, zarządzanie ryzykiem oraz wdrażanie odpowiednich środków zabezpieczających.
10. **Ochrona przed spoofingiem i atakami telefonicznymi** - mechanizmy ochrony przed spoofingiem, fałszowaniem numerów telefonów oraz innymi technikami oszustw telefonicznych.
11. **Bezpieczna komunikacja w środowisku cyfrowym** - szyfrowanie komunikacji, korzystanie z bezpiecznych kanałów komunikacyjnych, zabezpieczenie wideokonferencji oraz przesyłania danych.
12. **Ochrona przed wyłudzeniami danych osobowych (PII)** - zapobieganie wyłudzeniom danych osobowych za pomocą metod socjotechnicznych oraz przeciwdziałanie kradzieży tożsamości.

Zamawiający wymaga, aby Wykonawca wydał uczestnikom imienne certyfikaty oznaczone zgodnie z wymaganiami projektu Cyberbezpieczny Samorząd.

3/ przeprowadzenie szkolenia z zakresu bezpieczeństwa sieci komputerowych oraz Active Directory dla informatyka Urzędu Gminy Mirów

Zamawiający wymaga przeprowadzenia szkolenia dla informatyka Urzędu Gminy Mirów z zakresu bezpieczeństwa sieci komputerowych oraz Active Directory.

Zamawiający zezwalana na przeprowadzenia szkolenia w formie online, przy czym czas szkolenia nie może być krótszy niż 8 h szkoleniowych.

Zamawiający wymaga minimalnego zakresu szkolenia:

1. Instalacja i konfiguracja kontrolerów domeny

- Omówienie usług AD DS
- Omówienie kontrolerów domeny usług AD DS
- Wdrożenie kontrolera domeny
- Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server

2. Zarządzanie obiektami w AD DS

- Zarządzanie kontami użytkowników
- Zarządzanie grupami w usługach AD DS
- Zarządzanie obiektami typu komputer w AD DS
- Wdrażanie i zarządzanie OU

3. Zarządzanie zaawansowaną infrastrukturą AD DS

- Wprowadzenie do zaawansowanych wdrożeń AD DS
- Wdrożenie rozproszonego środowiska AD DS
- Konfiguracja relacji zaufania AD DS

4. Wdrażanie i zarządzanie lokacjami i repliką AD DS

- Omówienie replikacji usług AD DS
- Konfigurowanie lokacji usług AD DS
- Konfigurowanie i monitorowanie replikacji usług AD DS

5. Wdrażanie zasad grupy

- Wprowadzenie do zasad grupy
- Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)
- Konfiguracja zakresu i przetwarzania obiektów GPO
- Rozwiązywanie problemów z GPO

6. Zarządzanie ustawieniami użytkowników za pomocą zasad grupy

- Wdrażanie szablonów administracyjnych
- Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów
- Konfiguracja preferencji zasad grupowych