**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **Przedmiotem zamówienia jest przeprowadzenie audytu ochrony danych osobowych w siedzibie Zamawiającego, obejmującego m.in**.:

- weryfikację i ocenę organizacji systemu ochrony danych osobowych w Urzędzie,

- weryfikację i ocenę prawa do przetwarzania danych osobowych,

- weryfikację sposobu realizacji praw osoby, której dane dotyczą oraz jego ocenę,

- weryfikację i ocenę sposobu rejestrowania czynności przetwarzania danych osobowych,

- weryfikację i ocenę sposobu przeprowadzenia oceny skutków przetwarzania danych osobowych,

- weryfikację i ocenę procedur związanych z identyfikacją i zgłoszeniem naruszenia przetwarzania danych osobowych,

- wydanie rekomendacji w odniesieniu do obszarów wskazanych w pkt a - f, wskazujących na prawidłowe rozwiązania, w przypadku negatywnych praktyk – wskazanie sposobów ich rozwiązania,

- sporządzenie raportu kontroli zawierającego rekomendacje rozwiązań ewentualnych niezgodności.

**2. Techniki wykorzystane do przeprowadzenia audytu:**

1. badanie udostępnionych dokumentów i plików,

2. uzyskanie wyjaśnień od kierownictwa i pracowników administratora danych,

3. dokonanie oględzin obszarów przetwarzania danych osobowych w budynkach

Urzędu oraz na wybranych w uzgodnieniu z IOD 8 stanowiskach pracy.

1. **Zakres usługi w przedmiocie audytu bezpieczeństwa informacji we wszystkich obszarach funkcjonowania organizacji:**

Audyt organizacyjny obejmujący:

1. regulacje w obszarze zarządzania bezpieczeństwem informacji;
2. odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;
3. dokumentacja z zakresu ochrony danych osobowych;
4. przeprowadzenie wywiadów z wybranymi pracownikami.

Audyt fizyczny i środowiskowy obejmujący:

1. weryfikację granic obszaru bezpiecznego;
2. weryfikację zabezpieczeń wejścia/wyjścia;
3. weryfikację systemów zabezpieczeń pomieszczeń i urządzeń;
4. weryfikację bezpieczeństwa okablowania strukturalnego;
5. weryfikację systemów chłodzenia;
6. weryfikację systemów alarmowych.

Audyt ochrony danych osobowych obejmujący:

1. przegląd zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa;
2. przegląd istniejących regulacji wewnętrznych odnośnie bezpieczeństwa przetwarzania danych osobowych;
3. przegląd aktualnie wykorzystywanych dokumentów mających związek z ochroną danych osobowych;
4. identyfikację zbiorów podlegających rejestracji.

Audyt teleinformatyczny obejmujący:

1. weryfikację istniejących procedur zarządzania systemami teleinformatycznymi;
2. weryfikację ochrony przed oprogramowaniem szkodliwym;
3. weryfikację procedur zarządzania kopiami zapasowymi;
4. weryfikację procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
5. weryfikację zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe;
6. weryfikację haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania);
7. analizę i ocenę mechanizmów zarządzania aktualizacjami.

Zewnętrzne i wewnętrzne testy penetracyjne infrastruktury informatycznej obejmujące:

1. testy styku sieci lokalnej z internetem przeprowadzane ze stacji roboczej podłączonej do sieci internet;
2. analizę topologii brzegu sieci;
3. weryfikację mechanizmów ochronnych;
4. próbę wykrycia usług sieciowych udostępnianych do internetu;
5. detekcję wersji oraz typu oprogramowania dostępnego z sieci internet;
6. exploitację dostępnych urządzeń oraz usług wystawionych do sieci internet;
7. przedstawienie rozwiązań zwiększających bezpieczeństwo styku sieci lokalnej z siecią internet.

Testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji obejmujące :

1. analizę topologi sieci LAN;
2. weryfikację mechanizmów ochronnych w sieci;
3. analizę komunikacji sieciowej;
4. skanowanie portów TCP/UDP próba wykrycia usług sieciowych;
5. skanowanie hostów aktywnych w sieci;
6. exploitację dostępnych urządzeń oraz usług w sieci LAN;
7. przedstawienie rozwiązań zwiększających bezpieczeństwo w sieci LAN.

Badanie odporności użytkowników na socjotechniki.

Zakres testów socjotechnicznych obejmujący:

1. telefoniczny kontakt z użytkownikiem w celu próby pozyskania informacji niejawnych;
2. kontakt mailowy z próbami pozyskania danych logowania (phishing);
3. kontakt mailowy z próbami aktywowania wirusów / trojanów;
4. kontakt bezpośredni w celu uzyskania nieautoryzowanego dostępu do zasobów firmy;
5. próby podszycia się pod osobę znaną w celu nakłonienia do określonych działań zagrażających bezpieczeństwu.
6. **Wykonanie i przekazanie Raportów** z Audytu z omówieniem. Wskazanie obszarów niezgodności z RODO i zaproponowanie działań dostosowujących. Raport z zaleceniami należy sporządzić w wersji papierowej (3 egzemplarze) i na nośniku CD/DVD.
7. **Istotne informacje dotyczące realizacji audytu**:
   1. liczba pracowników: **64 osoby,**
   2. liczba lokalizacji: **3 budynki,**
   3. witryna internetowa <https://gminaolawa.pl/>,
   4. profil na portalu Facebook https://www.facebook.com/gminaOlawa,
   5. dokumentacja w zakresie ochrony danych osobowych:

* Polityka ochrony danych osobowych,
* Instrukcja zarządzania systemami informatycznymi,
* Rejestr czynności przetwarzana,
* Rejestr kategorii czynności przetwarzania,
* Analiza ryzyka ogólnego i ocena skutków dla przetwarzania danych (DPIA),
* Rejestr naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych,
* inne rejestry.