

Opis przedmiotu zamówienia

I. Przedmiotem zamówienia jest usługa polegająca na:

1. Przeprowadzeniu audytu:

- a) spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie KRI - Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w POSiR (zwanym dalej KRI);
- b) spełnienia wymogów Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 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 zwanych dalej RODO);
- c) spełnienia wymagań obowiązujących w POSiR regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI);
- d) bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych, które pozwolą ocenić aktualny stan bezpieczeństwa systemów Zamawiającego i określić obecność znanych podatności i odporności na próby przełamania stosowanych zabezpieczeń.

II. Cel audytu

1. Audyt w POSiR we wszystkich jego oddziałach (10 lokalizacji na terenie miasta Poznania) i działach (9 działów w Dyrekcji POSiR) którego celem jest:

- a) Weryfikacja poziomu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwanego dalej RODO,
- b) Weryfikacja poziomu spełnienia wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w POSiR, zwanego dalej KRI,
- c) Weryfikacja bezpieczeństwa systemu informatycznego Zamawiającego,
- d) Weryfikacja poziomu spełnienia wymagań obowiązujących w POSiR regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI).

III. Zakres audytu

Zakres audytu spełniania wymogów RODO, KRI oraz obowiązujących w POSiR regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI) oraz bezpieczeństwa systemu informatycznego Zamawiającego musi obejmować w szczególności:

1. Audyt organizacyjny polegający na:

a) weryfikacji środków organizacyjnych (w tym dokumentacja SZBI) w obszarze bezpieczeństwa informacji, w tym danych osobowych;

b) weryfikacji procesów i czynności przetwarzania danych uwzględniając ich charakter, zakres, kontekst, cele przetwarzania, zasoby, aktywa i ryzyka dla wszystkich oddziałów i działów POSiR;

c) weryfikacji realizowania przez pracowników POSiR obowiązków wynikających z regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI).

Wykaz obowiązków pracowników podlegających weryfikacji (poszczególnych procedur, instrukcji, zapisów z dokumentacji SZBI) zostanie przedłożony Wykonawcy po podpisaniu umowy.

Weryfikacja o której mowa w pkt. III.1 lit c) musi obejmować przynajmniej kierownika lub zastępcę kierownika każdej komórki organizacyjnej POSiR oraz 3 jej pracowników (chyba, że komórka posiada mniejszą liczbę pracowników – wówczas wszystkich jej pracowników).

Minimalny czas weryfikacji o której mowa w pkt. III.1 lit c) ustala się na 60 min. w przypadku kierownika lub zastępcy kierownika komórki organizacyjnej oraz 30 min. w przypadku pojedynczego pracownika. Nie dopuszcza się audytowania kilku pracowników jednocześnie przez jednego audytora.

2. Audyt fizyczny i środowiskowy polegający na

weryfikacji środków technicznych służących zabezpieczeniu informacji, w tym danych osobowych, w szczególności stanu bezpieczeństwa fizycznego i środowiskowego siedziby dyrekcji POSiR oraz wszystkich oddziałów POSiR (budynki oraz pomieszczenia) na podstawie wizji lokalnej obszarów przetwarzania danych.

3. Audyt teleinformatyczny polegający na:

a) przeprowadzeniu nieinwazyjnych (wewnętrznych i zewnętrznych) testów penetracyjnych systemów informatycznych Zamawiającego w szczególności odniesieniu do infrastruktury sieciowej, systemu Firewall, aplikacji, wszystkich serwisów www oraz poczty elektronicznej,

b) weryfikacji bezpieczeństwa infrastruktury sieciowej w szczególności:

- inwentaryzacja urządzeń sieciowych (adresy IP, konfiguracja urządzeń, konfiguracja zapory ogniowej, podział na sieci logiczne i fizyczne) w siedzibie dyrekcji Zamawiającego i wszystkich jego oddziałach;
- analiza urządzeń i ich parametrów technicznych zapewniających stronie Zamawiającej dostęp do sieci Internet - w tym serwera brzegowego, urządzeń UTM, Firewall, routerów;
- analiza konfiguracji sieci lokalnej;
- analiza oprogramowania wykorzystywanego przez Zamawiającego w zakresie zabezpieczenia informatycznego;
- analiza sposobu połączenia segmentów pomiędzy sobą;
- analiza metody komunikacji pomiędzy segmentami sieci.

c) weryfikacji bezpieczeństwa infrastruktury serwerowej w szczególności:

- analiza bezpieczeństwa zainstalowanych usług (czy zainstalowane oprogramowanie jest aktualne, czy zainstalowane oprogramowanie posiada znane luki w bezpieczeństwie, kto ma dostęp do udostępnionych usług);
- analiza bezpieczeństwa serwerów pod kątem dostępu użytkowników (czy jedynie uprawnieni użytkownicy mają dostęp do usług, czy udostępnione usługi zawierają jedynie te dane które są wymagane);
- analiza bezpieczeństwa uprawnień poszczególnych użytkowników oraz grup użytkowników;
- analiza bezpieczeństwa fizycznego infrastruktury serwerowej,

d) weryfikacji bezpieczeństwa poczty elektronicznej, domeny, stron internetowych zamawiającego,

e) weryfikacji bezpieczeństwa systemów (aplikacji) w których przetwarzane są dane osobowe w szczególności:

- analiza podatności komponentów aplikacji, w tym serwerów aplikacyjnych i baz danych - próby uzyskania dostępu do panelu administracyjnego za pomocą kont zwykłych użytkowników m. in. przez wykorzystanie bieżącej sesji, podniesienie uprawnień, próby uzyskania większych uprawnień, próby uzyskania nieautoryzowanego dostępu do danych znajdujących się w systemie;
- analiza szyfrowania danych dla danych przesyłanych przez sieci publiczne.

Wykaz systemów w których przetwarzane są dane osobowe w poszczególnych oddziałach i działach POSiR:

- dział FE (systemy księgowe, system obiegu faktur),
- dział DI (system zapisów na imprezy biegowe),
- dział DO (systemy płacowo-kadrowe, portal pracowniczy),
- oddziały ZS i GO (system Plaza),

- oddział RA (system Reserve),
- oddziały AT, KA, WI (system Fitnet),
- wszystkie oddziały i działy (system obiegu umów Redmine).

f) weryfikacji bezpieczeństwa stacji roboczych:

- analiza kontroli dostępu do stacji roboczych,
- analiza zainstalowanego oprogramowania znajdującego się na stacjach roboczych,
- analiza bezpieczeństwa stacji roboczych pod kątem zainstalowanych usług, dostępów zdalnych do stacji roboczych, bezpieczeństwa ochrony antywirusowej.

g) weryfikacji zarządzania kopiami zapasowymi i ciągłości działania w szczególności:

- analizę poprawności wykonywanych kopii zapasowych,
- analiza częstotliwości wykonywania kopii zapasowych,
- analiza bezpieczeństwa wykonywanych kopii zapasowych,
- analiza testów odzyskiwania kopii zapasowych – odtwarzania danych w środowisku testowym,
- analiza zbierania, przechowywania i monitorowania logów systemowych,

h) weryfikacji poprawności realizacji obowiązków wynikających z *Polityki bezpieczeństwa systemów informatycznych POSiR* oraz umowy o świadczenie usług przez Firmę IT obsługującą

Zamawiającego w szczególności w zakresie:

- zarządzania hasłami użytkowników i hasłami administracyjnymi,
- instalacji i aktualizacji oprogramowania,
- ochrony przed szkodliwym oprogramowaniem,
- zabezpieczania procesu pracy zdalnej,
- rozwoju systemów informatycznych,
- zarządzania zmianami w systemach informatycznych,
- przeglądów, konserwacji i napraw systemu informatycznego,
- monitorowania bezpieczeństwa systemów informatycznych w tym przy użyciu ZABBIX,
- zapisywanie, monitorowanie, zabezpieczanie logów systemowych,
- monitorowania pojemności i wydajności systemów informatycznych,
- bezpieczeństwa sieci,
- zapewnienia legalności oprogramowania,
- usuwania danych i niszczenia nośników,
- synchronizacji zegarów.

W czasie wykonania i po wykonaniu usługi infrastruktura Zamawiającego musi pozostać w niezmienionej formie, tj. nie może zostać uszkodzona, jak również nie mogą zostać usunięte, zmienione, nadpisane dane znajdujące się w tej infrastrukturze.

IV. Raport poaudytowy

Wynikiem przeprowadzonych audytów i testów będzie raport poaudytowy zawierający:

- a. przedmiot, cel i zakres audytu,
 - b. datę rozpoczęcia audytu,
 - c. opis przyjętej metodyki,
 - d. raport dla kierownictwa obejmujące syntezę wyników audytu i ocenę poziomu spełnienia wymogów RODO, KRI, regulacji wewnętrznych dot. bezpieczeństwa informacji Zamawiającego oraz ocenę bezpieczeństwa systemu informatycznego w tym podsumowanie zidentyfikowanych słabości/nieprawidłowości, a także główne rekomendacje dotyczące poprawy bezpieczeństwa informacji, danych i systemu informatycznego.
 - e. raport szczegółowy zawierający dokładny opis zidentyfikowanych nieprawidłowości w szczególności:
 - wskazujący dokładne miejsca, w których występują realne bądź potencjalne problemy z bezpieczeństwem informacji;
 - zawierający wyniki audytów, w tym testów i ich interpretację – każde ustalenie musi odnosić się do konkretnych przypadków słabości/nieprawidłowości popartych zgromadzonymi dowodami audytowymi, które będą stanowiły załącznik do raportu;
 - zawierający rekomendacje w zakresie eliminacji zidentyfikowanych słabości/nieprawidłowości oraz poprawy poziomu bezpieczeństwa, w tym wskazanie działań korygujących i/lub doskonalących.
- Ocena, ustalenia i rekomendacje muszą być ze sobą jasno powiązane i łatwo identyfikowalne.
- f. propozycje zmian w treści regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI) Zamawiającego wraz z proponowaną treścią nowych (zmienionych lub dodanych) zapisów;
 - g. datę sporządzenia raportu;
 - h. imiona i nazwiska audytorów realizujących zadanie oraz ich podpisy.

W terminie do 14 dni od daty zakończenia audytu w siedzibie Zamawiającego Wykonawca prześle w formie elektronicznej w formacie edytowalnym i pdf raport wstępny, zaszyfrowany programem 7 ZIP przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczony co najmniej 9-znakowym hasłem jednorazowym (zawierającym małe i duże litery, cyfry i znaki specjalne) przesłanym przez alternatywny kanał komunikacji.

Zamawiający ma prawo zgłoszenia uwag/zastrzeżeń do raportu wstępnego, do których Wykonawca ustosunkuje się w terminie wskazanym przez Zamawiającego, w tym nanosząc ewentualne korekty do raportu wstępnego.

Jeżeli Zamawiający nie będzie wnosił innych uwag/zastrzeżeń do skorygowanego raportu wstępnego poinformuje o tym Wykonawcę, który przygotuje na tej podstawie raport końcowy i przekaze go Zamawiającemu w terminie do 7 dni.

Wykonawca prześle raport końcowy w formie elektronicznej w formacie edytowalnym i pdf, zaszyfrowany w sposób opisany powyżej.

Wykonawca może dodatkowo przekazać raport końcowy w wersji edytowalnej w formacie A4 (druk dwustronny).

V. Zakres czasowy audytu

1. Czynności audytowe w siedzibie Zamawiającego powinny zakończyć się w ciągu 7 dni kalendarzowych od daty rozpoczęcia audytu w siedzibie Zamawiającego.

VI. Podstawowe informacje na temat systemów informatycznych Zamawiającego

1. liczba komputerów:

stacjonarnych - 127

przenośnych - 70

2. liczba serwerów:

fizycznych - 24

wirtualnych - 8

3. liczba aplikacji bazodanowych - systemów przetwarzających dane osobowe - 9

4. liczba serwerowni – 6 (Dyrekcja - serwerownia + kilka punktów dystrybucyjnych, Oddział RA, Oddział WI, Oddział MA - serwerownia + kilka punktów dystrybucyjnych, Oddział GO - serwerownia + kilka punktów dystrybucyjnych, Oddział ZS - serwerownia)

5. liczba urządzeń sieciowych – (drukarki, routery, switchy, voip, itd.) - 220

6. liczba Access Point - 40

7. liczba drukarek sieciowych - 50

8. liczba podsieci - 35

9. liczba adresów zewnętrznych – 23

10. wdrożony Active Directory w dyrekcji POSiR

11. liczba serwisów www - 6