Załącznik Nr 1

Gmina Miasto
Boguszów-Gorce

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA - CZĘŚĆ I

PRZEPROWADZENIE AUDYTU CYBERBEZPIECZEŃSTWA (DIAGNOZY CYBERBEZPIECZEŃSTWA) W URZĘDZIE MIEJSKIM W BOGUSZOWIE-GORCACH

realizowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020
Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU
działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia
dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi do przeprowadzenia kompleksowego audytu bezpieczeństwa informacji w zakresie ustawowych obszarów działalności podmiotu, w tym:

1. Audyt bezpieczeństwa danych w systemach informatycznych oraz sieci ICT:
   1) Analiza wszystkich zabezpieczeń przed utratą i kradzieżą danych
   2) Analiza kontroli dostępu do systemów informatycznych w tym dostępu przez usługi i narzędzia zdalne
   3) Analiza zabezpieczeń przy pracy zdalnej
   4) Analiza i ocena technicznej infrastruktury w systemach ICT, schematu sieci a także technicznych zabezpieczeń sieci.
   5) Analiza i ocena zabezpieczeń dostępu do sieci publicznej
   6) Analiza i ocena zabezpieczeń wewnętrznej sieci ICT
   7) Ocena sposobu identyfikowania i logowania użytkowników
   8) Analiza i ocena systemów backupów i archiwizacji danych w tym testy odtworzeniowe.
   9) Analiza i ocena ciągłości pracy systemów i sieci ICT
   10) Testy penetracyjne systemów informatycznych i całej infrastruktury ICT
   11) Sprawdzenie zabezpieczeń komputerów przed atakami phishingowymi
   12) Badanie podatności usług sieciowych
   13) Badanie podatności aplikacji serwera pocztowego email i aplikacji webowej zgodnie z OWASP.
   14) Weryfikacja systemu uwierzytelniania użytkowników i administratorów
   15) Weryfikacja systemu uwierzytelniania użytkowników i administratorów do systemu operacyjnego i kontrolera domeny
   16) Sprawdzenie sposobów i systemów szyfrowania m.in. protokoły szyfrowania, szyfrowanie danych END-to-END w poczcie email itp.
   17) Sprawdzenie i ocena szyfrowania danych przechowywanych poza Urzędem m.in. serwisy pocztowe email, serwisy WEB itp.
   18) Sprawdzenie systemów ochrony poczty email i usług WEB pod kątem ataków phishingowych
   19) Analiza i ocena sposobu zbierania logów, zakresu i retencji logów
   20) Identyfikacja pojedynczych punktów awarii

2. Audyt ochrony danych zgodnie z przepisami RODO, UODO, KRI, KSC
   1) Analiza zgodności dokumentacji ochrony danych osobowych
   2) Analiza upoważnień do przetwarzania danych osobowych
   3) Analiza umów powierzenia przetwarzania danych osobowych
   4) Analiza umów i porozumień dotyczących przekazywania danych osobowych
   5) Analiza rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania
   6) Ocena procesu zarządzania incydentami i reagowania na incydenty. Analiza informacji lub raportów dotyczących, incydentów naruszenia bezpieczeństwa danych
   7) Analiza konieczności dokonania oceny skutków dla planowanych sposobów przetwarzania danych
   8) Rozpoznanie roli i funkcji IODO
   9) Rozpoznanie wszystkich systemów przetwarzających dane i ich konfigurację
   10) Rozpoznanie wszystkich przetwarzanych zbiorów danych
   11) Kontrola zabezpieczeń zbiorów tradycyjnych
   12) Kontrola zabezpieczeń zbiorów archiwalnych
   13) Kontrola systemu monitoringu
   14) Kontrola systemu alarmowego
   15) Weryfikacja kontroli nad przepływem danych osobowych
   16) Weryfikacja poufności, dostępności i udostępniania danych osobowych
   17) Analiza i ocena zagrożeń z identyfikacją słabych stron związanych z przetwarzaniem danych
   18) Weryfikacja dostępu osób nieupoważnionych do miejsc, gdzie przetwarzane są dane
   19) Analiza i ocena procedur zarządzania systemami teleinformatycznymi
   20) Analiza i ocena zaangażowania Najwyższego Kierownictwa w proces ciągłego doskonalenia systemu bezpieczeństwa informacji
   21) Analiza i ocena ochrony ICT przed oprogramowaniem szkodliwym, w tym weryfikacja zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania
   22) Analiza i ocena procedur historii zmian w dokumentach, systemach informatycznych itp.
   23) Analiza i ocena procedur zarządzania i zabezpieczania nośników przechowujących dane
   24) Analiza i ocena zasad odpowiedzialności użytkowników
   25) Analiza i ocena zasad zarządzania hasłami
   26) Analiza i ocena zabezpieczeń kryptograficznych
   27) Analiza i ocena zabezpieczeń komputerów przenośnych w tym praca zdalna.
   28) Analiza stopnia zabezpieczenia stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe
   29) Analiza i ocena niszczenia niepotrzebnych nośników oraz danych
   30) Analiza i ocena stron webowych pod kątem zgodności standardu min. WCAG 2.1
3. Opracowanie raportu zawierającego ocenę stosowanych zabezpieczeń, analizę stanu bezpieczeństwa, wnioski, zalecenia i rekomendację dotyczące zakresu, metodyki i organizacji zabezpieczeń
4. Diagnoza cyberbezpieczeństwa w Urzędzie Miejskim w Boguszowie-Gorcach musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.) oraz Rozporządzeniem 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 (tj. Dz.U. 2017 poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI, w tym opracowanie raportu

zawierającego wnioski i rekomendacje oraz przeprowadzenie szkolenia w zakresie cyfrowego bezpieczeństwa pracowników Urzędu.

5. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronach Centrum Projektów Polska Cyfrowa [https://www.gov.pl/web/cppc/cyfrowa-gmina] - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - Załącznik Nr 8.
6. Audyt musi zostać przeprowadzony przez osobę posiadającą 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:
   1) Certified Internal Auditor (CIA)
   2) Certified Information System Auditor (CISA)
   3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PNEN 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
   4) 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
   5) Certified Information Security Manager (CISM)
   6) Certified in Risk and Information Systems Control (CRISC)
   7) Certified in the Governance of Enterprise IT (CGEIT)
   8) Certified Information Systems Security Professional (CISSP)
   9) Systems Security Certified Practitioner (SSCP)
   10) Certified Reliability Professional
   11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert
7. Diagnozę cyberbezpieczeństwa należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.

Załączniki do opisu diagnozy cyberbezpieczeństwa:

- Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa
- Rozporządzenie Mini._Cyfryzacji_wykaz_certyfikatów_uprawniających_do_przeprowadzenia_audytu