

Projekt współfinansowany w ramach umowy o powierzenie grantu o numerze 316/1/2021 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

Załącznik nr 2

Szczegółowy opis wymagań diagnozy cyberbezpieczeństwa:

1. Audyt bezpieczeństwa danych w systemach informatycznych oraz sieci ICT:
 - 1.1 Analiza wszystkich zabezpieczeń przed utratą i kradzieżą danych
 - 1.2 Analiza kontroli dostępu do systemów informatycznych w tym dostępu przez usługi i narzędzia zdalne
 - 1.3 Analiza zabezpieczeń przy pracy zdalnej
 - 1.5 Analiza i ocena technicznej infrastruktury w systemach ICT, schematu sieci a także technicznych zabezpieczeń sieci.
 - 1.6 Analiza i ocena zabezpieczeń dostępu do sieci publicznej
 - 1.7 Analiza i ocena zabezpieczeń wewnętrznej sieci ICT
 - 1.8 Ocena sposobu identyfikowania i logowania użytkowników
 - 1.9 Analiza i ocena systemów backupów i archiwizacji danych w tym testy odtworzeniowe.
 - 1.10 Analiza i ocena ciągłości pracy systemów i sieci ICT
 - 1.11 Testy penetracyjne systemów informatycznych i całej infrastruktury ICT
 - 1.12 Sprawdzenie zabezpieczeń komputerów przed atakami phishingowymi
 - 1.13 Badanie podatności usług sieciowych
 - 1.14 Badanie podatności aplikacji serwera pocztowego email i aplikacji webowej zgodnie z OWASP.
 - 1.15 Weryfikacja systemu uwierzytelniania użytkowników i administratorów
 - 1.16 Weryfikacja systemu uwierzytelniania użytkowników i administratorów do systemu operacyjnego i kontrolera domeny
 - 1.17 Sprawdzenie sposobów i systemów szyfrowania m.in. protokoły szyfrowania, szyfrowanie danych END-to-END w poczcie email itp.
 - 1.18 Sprawdzenie i ocena szyfrowania danych przechowywanych poza Urzędem m.in. serwisy pocztowe email, serwisy WEB itp.
 - 1.19 Sprawdzenie systemów ochrony poczty email i usług WEB pod kątem ataków phishingowych
 - 1.20 Analiza i ocena sposobu zbierania logów, zakresu i retencji logów
 - 1.21 Identyfikacja pojedynczych punktów awarii
2. Audyt ochrony danych zgodnie z przepisami RODO, UODO, KRI, KSC:
 - 2.1 Analiza zgodności dokumentacji ochrony danych osobowych
 - 2.2 Analiza upoważnień do przetwarzania danych osobowych
 - 2.3 Analiza umów powierzenia przetwarzania danych osobowych
 - 2.4 Analiza umów i porozumień dotyczących przekazywania danych osobowych
 - 2.5 Analiza rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania
 - 2.6 Ocena procesu zarządzania incydentami i reagowania na incydenty. Analiza informacji lub raportów dotyczących, incydentów naruszenia bezpieczeństwa danych
 - 2.7 Analiza konieczności dokonania oceny skutków dla planowanych sposobów przetwarzania danych
 - 2.8 Rozpoznanie roli i funkcji IODO
 - 2.9 Rozpoznanie wszystkich systemów przetwarzających dane i ich konfigurację

Projekt współfinansowany w ramach umowy o powierzenie grantu o numerze 316/1/2021 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

- 2.10 Rozpoznanie wszystkich przetwarzanych zbiorów danych
 - 2.11 Kontrola zabezpieczeń zbiorów tradycyjnych
 - 2.12 Kontrola zabezpieczeń zbiorów archiwalnych
 - 2.13 Kontrola systemu monitoringu
 - 2.14 Kontrola systemu alarmowego
 - 2.15 Weryfikacja kontroli nad przepływem danych osobowych
 - 2.16 Weryfikacja poufności, dostępności i udostępniania danych osobowych
 - 2.17 Analiza i ocena zagrożeń z identyfikacją słabych stron związanych z przetwarzaniem danych
 - 2.18 Weryfikacja dostępu osób nieupoważnionych do miejsc, gdzie przetwarzane są dane
 - 2.19 Analiza i ocena procedur zarządzania systemami teleinformatycznymi
 - 2.20 Analiza i ocena zaangażowania Najwyższego Kierownictwa w proces ciągłego doskonalenia systemu bezpieczeństwa informacji
 - 2.21 Analiza i ocena ochrony ICT przed oprogramowaniem szkodliwym, w tym weryfikacja zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania
 - 2.22 Analiza i ocena procedur historii zmian w dokumentach, systemach informatycznych itp.
 - 2.23 Analiza i ocena procedur zarządzania i zabezpieczania nośników przechowujących dane
 - 2.24 Analiza i ocena zasad odpowiedzialności użytkowników
 - 2.25 Analiza i ocena zasad zarządzania hasłami
 - 2.26 Analiza i ocena zabezpieczeń kryptograficznych
 - 2.27 Analiza i ocena zabezpieczeń komputerów przenośnych w tym praca zdalna.
 - 2.28 Analiza stopnia zabezpieczenia stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe
 - 2.29 Analiza i ocena niszczenia niepotrzebnych nośników oraz danych
 - 2.30 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.
- 4.1 Diagnoza cyberbezpieczeństwa 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.
 - 4.2
Diagnoza cyberbezpieczeństwa musi zostać wykonana 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.

Projekt współfinansowany w ramach umowy o powierzenie grantu o numerze 316/1/2021 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

4.3 Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona 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:

- a) Certified Internal Auditor (CIA);
- b) Certified Information System Auditor (CISA);
- c) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN 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;
- d) 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;
- e) Certified Information Security Manager (CISM) ;
- f) Certified in Risk and Information Systems Control (CRISC) ;
- g) Certified in the Governance of Enterprise IT (CGEIT) ;
- h) Certified Information Systems Security Professional (CISSP) ;
- i) Systems Security Certified Practitioner (SSCP) ;
- j) Certified Reliability Professional ;
- k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

5. Wynikiem diagnozy cyberbezpieczeństwa jest:

1. pełny raport z przeprowadzonej diagnozy;
2. rekomendacje dotyczące technicznych zabezpieczeń danych i informacji;
3. opracowanie dokumentu oceny ryzyka;
4. opracowanie procedur dotyczących bezpieczeństwa;
5. opracowanie i wdrożenie SZBI;
6. przeszkolenie pracowników z wdrożonego systemu SZBI i procedur związanych z bezpieczeństwem.

Termin wykonania przedmiotu zamówienia : do 13 czerwca 2022 r.

Wykonawca zobowiązuje się do wykonania (w ramach proponowanej ceny) **do wykonania reaudytu** w obszarach które uległy zmianom w trakcie wdrożenia projektu „Cyfrowa Gmina” w terminie do **30 dni od zakończenia działań w projekcie „Cyfrowa Gmina”**.