

Załącznik nr 1

Znak sprawy: ROO.271.4.2026

OPIS PRZEDMIOTU ZAMÓWIENIA**1.1 Przeprowadzenie audytu bezpieczeństwa informacji początkowego i końcowego w ramach realizacji projektu „Cyberbezpieczny Samorząd”**

Przeprowadzenie audytów bezpieczeństwa (początkowego i końcowego):

Przeprowadzanie audytów (początkowego i końcowego) w zgodności z KRI oraz Ustawy o Krajowym Systemie Cyberbezpieczeństwa dla Urzędu Gminy w Stoszowicach. Opracowanie raportu z audytu wraz z rekomendacjami do wdrożenia w ramach projektu „Cyberbezpieczny Samorząd”. Omówienie wyników audytu w siedzibie Zamawiającego.

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do zapewnienia:

- a) Realizacji audytu bezpieczeństwa informacji w siedzibie Zamawiającego (nie jest przewidziana zdalna realizacja);
- b) Zapewnienia zgodności realizowanego audytu bezpieczeństwa informacji z następującymi wymaganiami:
 - i. Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych- Ustawy o Krajowym Systemie Cyberbezpieczeństwa;
 - ii. Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
 - iii. wymagań określonych w normie ISO 27001.
- c) Opracowanie raportu z audytu wraz z rekomendacjami do wdrożenia w ramach projektu „Cyberbezpieczny Samorząd”, w szczególności w odniesieniu do wyników ankiety wypełnionej przez Zamawiającego, zgodnie z regulaminem projektu „Cyberbezpieczny Samorząd”;
- d) Omówienie wyników audytu w siedzibie Zamawiającego.

Szczegółowy zakres audytu powinien objąć następujące obszary:

- a) prawidłowości prowadzonej przez Zamawiającego dokumentacji aktualnej oraz planowanej, dotyczącej Systemu Zarządzania Bezpieczeństwa Informacji w zakresie jego poufności, dostępności i integralności informacji,
- b) zapewniania przez Zamawiającego aktualizacji regulacji wewnętrznych w zakresie, dotyczącym zmieniającego się otoczenia,
- c) utrzymywania przez Zamawiającego aktualności inwentaryzacji sprzętu i oprogramowania, służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,
- d) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
- e) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,
- f) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji z uwzględnieniem aspektów związanych z bezpieczeństwem informacji,
- g) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
- h) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
- i) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,
- j) ustalonych zapisów zawieranych w umowach serwisowych gwarantujących odpowiedni poziom bezpieczeństwa informacji,
- k) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
- l) zapewnienia odpowiedniego określonego przez KRI poziomu bezpieczeństwa w systemach teleinformatycznych,

- m) sposobu postępowania z incydentami związanymi z bezpieczeństwem informacji, w tym bezzwłocznego zgłaszania takich incydentów,
- n) przeglądu zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa,
- o) przeglądu istniejących regulacji wewnętrznych odnośnie bezpieczeństwa przetwarzania danych osobowych,
- p) przeglądu aktualnie wykorzystywanych dokumentów mających związek z ochroną danych osobowych,
- q) weryfikacji istniejących procedur zarządzania systemami teleinformatycznymi,
- r) weryfikacji ochrony przed oprogramowaniem szkodliwym,
- s) weryfikacji procedur zarządzania kopiami zapasowymi,
- t) weryfikacji procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
- u) weryfikacji zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
- v) weryfikacji haseł,
- w) analizy i oceny mechanizmów zarządzania aktualizacjami.

1.2 Opracowanie, aktualizacja dokumentacji, Systemu Zarządzania Bezpieczeństwem Informacji.

Przedmiotem zamówienia jest aktualizacja istniejącej dokumentacji i wdrożenie - opracowanie kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w ramach projektu „Cyfrowy Samorząd”

Zakres zadania obejmuje czynności związane z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji, zgodnego z poniższymi wymaganiami:

- a) rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
- b) ustawa z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;

c) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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);

d) wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;

e) wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd”.

Szczegółowy zakres dokumentacji powinien składać się z następujących obszarów:

- a. zarządzanie aktywami,
- b. zarządzanie ryzykiem,
- c. zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
- d. zapewnienie bezpieczeństwa fizycznego,
- e. kontrola dostępu do oprogramowania i infrastruktury sieciowej,
- f. klasyfikacja informacji oraz nadzoru nad dokumentacją,
- g. zapewnienie bezpieczeństwa zasobów ludzkich,
- h. wykonywanie kopii zapasowych,
- i. stosowanie kryptografii,
- j. obsługa incydentów i realizacja działań korygujących,
- k. prowadzenie wewnętrznych audytów bezpieczeństwa,
- l. prowadzenie przeglądów zarządzania,
- m. zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
- n. zapewnienie bezpieczeństwa łańcucha dostaw,
- o. postępowanie z podatnościami systemów i sieci,
- p. Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).

W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022.

1.3 Szkolenie z zakresu SZBI:

Przeprowadzenie stacjonarnego szkolenia w Urzędzie Gminy Stoszowice z zakresu bezpieczeństwa informacji odpowiednio do zdefiniowanych w SZBI ról oraz stanowisk pracy objętych zasięgiem działania SZBI w UG Stoszowice. W zakres szkolenie będą wchodzić metody ciągłego doskonalenia (aktualizowania) SZBI - audyty oraz działania korygujące. Liczba osób które zostaną przeszkolone - 2 pracowników Urzędu Gminy Stoszowice.

Do przeprowadzenia szkoleń Zamawiający udostępni salę szkoleniową w siedzibie Zamawiającego, udostępni projektor oraz ekran. Przygotowanie ewentualnej pozostałej infrastruktury szkoleniowej jest w gestii Wykonawcy i powinno być dostosowane do rodzaju szkolenia i liczby osób skierowanych na szkolenia, w szczególności dotyczy to (uzgodnionego) programu szkolenia, materiałów szkoleniowych, a także dokumentacji z przeprowadzonych szkoleń w tym listy obecności.

Zamawiający zakłada, iż minimalna liczba godzin na pakiet szkolenia to minimum 4 pełne godziny szkolenia, przy czym podany czas jest wyłącznie oceną Zamawiającego i nie powinien ograniczać Wykonawcy w możliwości efektywnego przeprowadzenia szkolenia w większej liczbie godzin, jeżeli zakres i licznosc zagadnień wymaga takiego zwiększenia liczby godzin.

1.4 Szkolenia z cyberbezpieczeństwa dla pracowników Urzędu Gminy

Przeprowadzenie szkolenia stacjonarnego dla 21 pracowników Urzędu Gminy w Stoszowicach z zakresu cyberbezpieczeństwa. Opracowanie poradnika z zakresu cyberbezpieczeństwa dla pracowników, który zostanie przekazany w formie tekstowej oraz graficznej, poradnik dostosowany będzie pod kątem wymogów dostępności dla osób o szczególnych potrzebach

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do:

1. Przygotowanie i przeprowadzenie szkoleń dla pracowników z zakresu cyberbezpieczeństwa.
2. Opracowanie poradnika z zakresu cyberbezpieczeństwa dla pracowników, który zostanie przekazany w formie tekstowej oraz graficznej, dostosowanej pod kątem wymogów dostępności dla osób o szczególnych potrzebach.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z przygotowaniem i przeprowadzeniem szkoleń dla pracowników z zakresu cyberbezpieczeństwa:

1. W ramach wykonywanych prac materiał szkoleniowy zaprezentowany przez Wykonawcę będzie odwoływał się do poniższych wymagań prawnych:
 - a. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO);
 - b. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
 - c. ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
 - d. rozporządzenia Rady Ministrów z dnia 21 maja 2014 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
 - e. ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami;
 - f. ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych;
 - g. wytycznych CSIRT NASK.
2. Przeprowadzanie szkolenie pracowników odbędzie się stacjonarnie i będzie obejmowało następujące obszary:
 - 1) Bezpieczeństwo informacji w ramach wykorzystywania oprogramowania i przetwarzania danych osobowych:
 - a. Zasady przetwarzania danych osobowych.
 - b. Prawa osób w kontekście ochrony danych osobowych.
 - c. Skutki naruszenia zasad oraz zarządzanie naruszeniami.
 - d. Sposoby zapewnienia bezpieczeństwa informacji u Zamawiającego.

- e. Zapewnienie ochrony prywatności w przeglądarkach internetowych.
- f. Dostępność cyfrowa w sieci oraz oprogramowaniu.
- g. Realizowanie zasad związanych z dostępnością dla osób ze szczególnymi potrzebami z wykorzystaniem oprogramowania w celu zapewnienia bezpieczeństwa informacji.

2) Zasady cyberbezpieczeństwa w ramach wykonywanej pracy zapewniające bezpieczeństwo zasobów jednostki:

- h. Czym jest phishing?
- i. Czym jest ransomware?
- j. Socjotechnika jako podstawowe narzędzie sprawców ataków.
- k. Zasady bezpiecznego korzystania z Internetu;
- l. Zasady bezpiecznego korzystania z poczty elektronicznej i zagrożenia z tym związane;
- m. Zasady bezpiecznego korzystania z haseł;
- n. Zagrożenia bezpieczeństwa informacji przy korzystaniu z sieci Internet.
 - i. Ataki przez pocztę e-mail
 - ii. Ataki przez strony WWW
 - iii. Bezpieczna praca z przeglądarką internetową
- o. Bezpieczna praca z programem pocztowym
- p. Bezpieczne korzystanie z sieci bezprzewodowych (Wi-Fi, Bluetooth).
- q. Zagrożenia i sposoby zabezpieczania sprzętu mobilnego;
- r. Korzystanie z menedżera haseł w praktyce;
- s. Przykłady technik stosowanych przez cyberprzestępców;
- t. Zasady bezpiecznego realizowania pracy zdalnej.
- u. Wycieki informacji – mechanizmy i skutki.
- v. Zarządzanie hasłami – dobre praktyki i narzędzia pomocnicze.
- w. Psychomanipulacja w sieci – zasady i zastosowania.
- x. Sfałszowane komunikaty i strony – identyfikacja zagrożeń.
- y. Ataki głosowe i podszywanie się pod identyfikator dzwoniącego (vishing).
- z. Deepfake oraz inne zagrożenia wynikające ze stosowania AI w przyszłości.
- aa. Mechanizmy ochronne przed cyberzagrożeniami.

3. Realizowane szkolenie będzie mieć formę stacjonarną, realizowaną w siedzibie Zamawiającego, dla dwóch grup pracowników, przy czym każda grupa będzie się składała z minimum 9 osób, a łączna ilość osób do przeszkolenia wynosi 21
4. Czas trwania jednego szkolenia (grupy) wynosi 3,5 godziny.
5. Zamawiający udostępni salę do prowadzenia wszystkich szkoleń stacjonarnych.
6. Wykonawca opracuje i wyda każdemu z uczestników szkoleń imienny certyfikat uczestnictwa w szkoleniach, który będzie oznaczony zgodnie z zasadami wizualizacji programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC).

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z opracowaniem poradnika z zakresu cyberbezpieczeństwa dla pracowników, który zostanie przekazany w formie tekstowej oraz graficznej, dostosowanej pod kątem wymogów dostępności dla osób o szczególnych potrzebach (punkt numer 4):

1. Wykonawca zobowiązany jest do opracowania poradnika z zakresu cyberbezpieczeństwa dla pracowników, który w sposób przystępny, z wykorzystaniem elementów graficznych będzie przedstawiał podstawowe zasady z zakresu bezpieczeństwa informacji i podejmowania działań związanych z należytą ochroną informacji.
2. Poradnik powinien składać się minimum z następujących zagadnień:
 - a. Bezpieczne korzystanie z oprogramowania.
 - b. Zasady aktualizacji programów i aplikacji.
 - c. Szyfrowanie dokumentów i poczty elektronicznej.
 - d. Polityka haseł oraz zarządzanie dostępem.
 - e. Zasady bezpiecznej pracy zdalnej.
 - f. Bezpieczna praca z plikami.
3. Poradnik objętościowo powinien mieć od minimum 5 stron A4 do 15 stron A4.
4. Poradnik powinien zostać opracowany w formie elektronicznej w pliku pdf.
5. Przekazywany plik powinien być dostosowany do potrzeb osób o szczególnych potrzebach, zgodnie z wymogami ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami.