Załącznik nr 1 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

I. **Wykonanie audytu (diagnozy)** powinno się odbyć zgodnie z następującymi przepisami:

 - 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

 (Dz. U. z 2017 r., poz. 2247 z późn. zm.),

 - Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dzu. U. z 2018 r., poz. 1560 z późn. zm.),

 - Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu

 Wykonana diagnoza powinna być zgodna z zakresem oraz formularzem stanowiącym załącznik

 nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina opublikowanego na stronie Centrum

 Projektów Polska Cyfrowa pod adresem https:/ / www.gov.p1/ web/cppc/cyfrowa¬gmina oraz

 zgodna z zapisami umowy o powierzenie grantu.

 W ramach zamówienia Wykonawca zobowiązany jest do przeprowadzenia diagnozy cyberbezpieczeństwa w siedzibie Zamawiającego – przynajmniej 2 dni pracy w siedzibie Zamawiajacego.

 Zamawiajacy nie dopuszcza możliwości realizacji usługi za pomocą środków zdalnej komunikacji.

II. **Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji** **(SZBI)** opartego o normę

 ISO 27001, które powinno zawierać następujące elementy :

1. Określenie ról i odpowiedzialności w zarządzaniu bezpieczeństwem informacji

1.1. Najwyższe kierownictwo i odpowiedzialność za zarządzanie bezpieczeństwem informacji

1.2. Role związane z Systemem Zarządzania Bezpieczeństwem Informacji

2. Odpowiednio zdefiniowana i wdrożona struktura dokumentacji definiującej zarządzanie

 bezpieczeństwem informacji

2.1. Charakter obecnie obowiązującej dokumentacji

2.2. Wdrożenie nowej lub aktualizacja obecnej dokumentacji

2.3. Nadzorowanie dokumentacji

2.4. Nadzorowanie zapisów

3. Zdefiniowane mechanizmy doskonalenia wykorzystywane w zarządzaniu bezpieczeństwem

 informacji

3.1. Audyty wewnętrzne

3.2. Działania korygujące / zapobiegawcze

3.3. Przeglądy Zarządzania

3.4. Incydenty Bezpieczeństwa

4. Wdrożony proces oceny ryzyka

4.1. Identyfikacja zasobów

4.2. Klasyfikacja informacji

4.3. Ocena ryzyka dla zasobu

4.4. Szacowanie ryzyka

4.5. Plan działań doskonalących

4.6. Wykorzystanie mechanizmów ciągłego doskonalenia do nadzorowania bezpieczeństwa i

 informacji.

 Wynikiem wykonania i wdrożenia SZBI opartego na normie ISO 27001 powinny być :

- pełny raport zawierający: ocenę stosowanych zabezpieczeń, analizę stanu bezpieczeństwa,

 wnioski,

- rekomendacje dotyczące technicznych zabezpieczeń danych i informacji,

- opracowanie dokumentu oceny ryzyka,

- opracowanie procedur dotyczących bezpieczeństwa

III. **Przeprowadzenie szkolenia** dla urzędników w zakresie cyberbezpieczeństwa, dotyczącego praktycznego stosowania mechanizmów bezpieczeństwa korespondencji i zabezpieczenia danych.

 Szkolenie powinno składać się z części teoretycznej i praktycznej.

 Wymagania dotyczące organizacji szkolenia:

 - szkolenie odbędzie się w siedzibie Zamawiającego w trybie stacjonarnym oraz na platformie

 e-learningowej w trybie zdalnym,

 - w szkoleniu będzie brało udział 30 osób - jedna grupa szkoleniowa,

 - szkolenie będzie prowadzone w języku polskim,

 - Wykonawca zapewni materiały szkoleniowe, w odpowiedni sposób oznakowane,

 - każdy uczestnik szkolenia otrzyma zaświadczenie/certyfikat o ukończeniu szkolenia,

 - Wykonawca zapewni kadrę trenerską posiadającą wiedzę, doświadczenie i umiejętności

 adekwatne do rodzaju i zakresu merytorycznego szkolenia.

 - Wykonawca zobowiązany jest do przekazania dokumentacji szkolenia Zamawiającemu w formie

 papierowej (dokumentacja fotograficzna w formie elektronicznej).

 - Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem

 przedmiotu zamówienia, w tym koszty swojego ewentualnego zakwaterowania, dojazdu,

 wyżywienia, wydruku i skanu dokumentów. Wyżywienie podczas szkolenia każdy uczestnik

 zapewnia sobie we własnym zakresie.

IV. **Utworzenie portalu** – witryny internetowej

Wykonawca powinien zapewnić pełna zgodność z wytycznymi WCAG 2.1.

Domena powinna być zabezpieczona certyfikatem SSL.