Zamawiający:
Gmina Ożarowice

Załącznik nr 1 – Opis przedmiotu zamówienia
Dot. zapytania ofertowego nr **ROI.271.5.2025**

OPIS PRZEDMIOTU ZAMÓWIENIA:

Dotyczy usług:

1. **<u>Przeprowadzenie szkolenia dla kadry kierowniczej Urzędu Gminy Ożarowice, Ośrodka Pomocy Społecznej w Ożarowicach, Zakładu Gospodarki Komunalnej w Ożarowicach, z zakresu Systemu Zarządzania Bezpieczeństwem Informacji</u>**

Zamawiający wymaga przeprowadzenia szkolenia stacjonarnego z zakresu Systemu Zarządzania Bezpieczeństwem Informacji. Zamawiający dopuszcza możliwość przeprowadzenia szkolenia w grupie łączonej (wspólnie dla kadry kierowniczej Urzędu Gminy Ożarowice, Ośrodka Pomocy Społecznej w Ożarowicach, Zakładu Gospodarki Komunalnej w Ożarowicach) w terminie opisanym w zapytaniu ofertowym.

Ilość pracowników (kadry kierowniczej) na szkoleniu z SZBI:
- Urzędu Gminy Ożarowice: **4**
- Ośrodka Pomocy Społecznej w Ożarowicach: **2**
- Zakładu Gospodarki Komunalnej w Ożarowicach: **3**

Zakres omawianej tematyki na szkoleniu wymieniony poniżej może być uzupełniony przez Wykonawcę o inne istotne aspekty. Wymagany czas trwania szkolenia **minimum 3,5 godziny**. Zamawiający wymaga, aby podczas szkolenia poruszone zostały kluczowe aspekty SZBI, w tym m.in.:

a. **Wprowadzenie do Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):**
- definicja i znaczenie SZBI;
- podstawowe pojęcia związane z bezpieczeństwem informacji;
- przegląd normy ISO/IEC 27001:2023;
- kluczowe elementy SZBI i ich rola w organizacji;

b. **Polityka Bezpieczeństwa Informacji:**
- definicja i cel Polityki Bezpieczeństwa Informacji;
- tworzenie, wdrażanie i utrzymanie polityki bezpieczeństwa;
- rola kadry kierowniczej w zarządzaniu polityką bezpieczeństwa;

c. **Zarządzanie ryzykiem:**
- proces identyfikacji, analizy i oceny ryzyka;
- metodyka oceny ryzyka zgodnie z ISO/IEC 27005;
- implementacja i monitorowanie środków kontrolnych;

d. **Zarządzanie incydentami bezpieczeństwa:**
- definicja incydentu bezpieczeństwa i jego rodzaje;
- procedury raportowania i reagowania na incydenty;
- role i odpowiedzialności w zarządzaniu incydentami;
- przykłady praktycznych scenariuszy incydentów;

e. **Kontrola dostępu i zarządzanie tożsamością:**
- zasady kontroli dostępu w organizacji;
- bezpieczne zarządzanie tożsamością użytkowników;
- autoryzacja, autentykacja i monitorowanie aktywności;

f. **Świadomość i szkolenia Pracowników:**
- rola edukacji i szkoleń w zapewnieniu bezpieczeństwa informacji;
- tworzenie programu szkoleń z zakresu bezpieczeństwa informacji;
- praktyczne wskazówki dotyczące podnoszenia świadomości pracowników;

g. **Audyt i monitorowanie systemu:**
- procedury audytu wewnętrznego SZBI;
- monitorowanie i przegląd efektywności systemu;
- rola kadry kierowniczej w zapewnieniu zgodności z wymaganiami;

h. **Zarządzanie ciągłością działania:**
- planowanie i wdrażanie strategii ciągłości działania;
- testowanie i aktualizacja planów ciągłości;
- integracja zarządzania ciągłością działania z SZBI;

i. **Przepisy prawne i regulacyjne:**
- przegląd kluczowych przepisów prawa dotyczących ochrony danych i bezpieczeństwa informacji;
- obowiązki urzędów gminnych w zakresie zgodności z przepisami;
- zarządzanie zgodnością z RODO i innymi regulacjami;

j. **Rola i odpowiedzialność kadry kierowniczej**
- kluczowe zadania kadry kierowniczej w zakresie zarządzania bezpieczeństwem informacji;
- budowanie kultury bezpieczeństwa w organizacji;
- motywowanie i nadzorowanie zespołów odpowiedzialnych za SZBI.

2. **<u>Przeprowadzenie szkoleń dla pracowników Urzędu Gminy Ożarowice, Ośrodka Pomocy Społecznej w Ożarowicach, Zakładu Gospodarki Komunalnej w Ożarowicach z zakresu cyberbezpieczeństwa.</u>**

Zamawiający wymaga przeprowadzenia dwóch szkoleń stacjonarnych z zakresu cyberbezpieczeństwa (pierwsze w 2025r, drugie w 2026r), w terminach opisanych w zapytaniu ofertowym. Ze względu na specyfikę pracy jednostek administracji publicznej, szkolenie musi zostać podzielone na dwie grupy, tak aby w danym dniu mogło w nim uczestniczyć

maksymalnie 50% kadry. Zamawiający dopuszcza realizację szkoleń tego samego dnia dla dwóch grup (w różnych godzinach) i w tym samym miejscu, jednocześnie dla pracowników kilku jednostek administracji publicznej biorących udział w projekcie. Zakres omawianej tematyki na szkoleniach może być uzupełniony przez Wykonawcę o inne istotne aspekty. Wymagany czas trwania jednego szkolenia – **minimum 3,5 godziny.**

Ilość pracowników na szkoleniach z zakresu cyberbezpieczeństwa:
- Urzędu Gminy Ożarowice **30**
- Ośrodka Pomocy Społecznej w Ożarowicach: **8**
- Zakładu Gospodarki Komunalnej w Ożarowicach **25**

Po przeprowadzeniu pierwszego oraz drugiego szkolenia dla pracowników z zakresu cyberbezpieczeństwa, Wykonawca zobowiązany jest do weryfikacji poziomu wiedzy przyswojonej przez uczestników. Weryfikacja powinna mieć formę testu wiedzy w formie pisemnej, obejmującego zagadnienia omawiane podczas szkoleń. Wyniki testu należy udokumentować w formie zbiorczego raportu zawierającego co najmniej: liczbę uczestników biorących udział w teście, średni wynik uzyskany przez uczestników, analizę obszarów wymagających dalszego doskonalenia. Raport z weryfikacji wiedzy należy przekazać Zamawiającemu w terminie do 14 dni od daty zakończenia szkolenia.

Zakres tematyki omawianej na szkoleniu:
1. **Wprowadzenie do cyberbezpieczeństwa -** definicja i znaczenie cyberbezpieczeństwa w administracji publicznej. Omówienie roli i odpowiedzialności pracowników w utrzymaniu bezpieczeństwa informacji.
2. **Podstawowe zasady cyberbezpieczeństwa** - omówienie fundamentalnych reguł i procedur dotyczących ochrony danych, zarządzania hasłami, autoryzacji i bezpiecznego korzystania z zasobów informatycznych.
3. **Phishing i inne ataki socjotechniczne** - rozpoznawanie i ochrona przed próbami wyłudzenia informacji, atakami phishingowymi oraz innymi technikami socjotechnicznymi.
4. **Zagrożenia związane z oprogramowaniem typu ransomware i malware** - identyfikacja, mechanizmy działania oraz metody zapobiegania i reagowania na zagrożenia związane z ransomware i malware.
5. **Bezpieczna obsługa poczty elektronicznej** - zasady korzystania z e-maila, rozpoznawanie podejrzanych wiadomości, załączników oraz linków, a także ochrona przed spamem i phishingiem.
6. **Zarządzanie hasłami i autoryzacja** - tworzenie silnych haseł, korzystanie z menedżerów haseł, wprowadzenie autoryzacji dwuetapowej oraz znaczenie kluczy sprzętowych.
7. **Ochrona urządzeń mobilnych - zabezpieczanie urządzeń przenośnych przed utratą danych, kradzieżą oraz złośliwym oprogramowaniem.**
8. **Bezpieczne przetwarzanie i przechowywanie danych** - szyfrowanie danych, zasady bezpiecznego przechowywania informacji, zarządzanie dostępem oraz udostępnianie danych w sposób bezpieczny.

9. **Zarządzanie dostępem do systemów i informacji** - zasady przydzielania uprawnień, kontrola dostępu oraz monitorowanie aktywności użytkowników w systemach informacyjnych.
10. **Bezpieczna komunikacja w środowisku cyfrowym** - szyfrowanie komunikacji, korzystanie z bezpiecznych kanałów komunikacyjnych, zabezpieczenie wideokonferencji oraz przesyłania danych.
11. **Ochrona przed wyłudzeniami danych osobowych (PII)** - zapobieganie wyłudzeniom danych osobowych za pomocą metod socjotechnicznych oraz przeciwdziałanie kradzieży tożsamości.
12. **Reagowanie na incydenty bezpieczeństwa** - procedury postępowania w przypadku incydentu, raportowanie naruszeń, analizowanie przyczyn oraz minimalizowanie skutków.
13. Podsumowanie szkolenia

3. Dostawa platformy edukacyjno-szkoleniowej w zakresie cyberbezpieczeństwa

Zamawiający wymaga dostarczenia platformy edukacyjno-szkoleniowej służącej do symulacji zagrożeń internetowych wraz z kompleksowym wsparciem technicznym. System ma na celu podniesienie świadomości użytkowników w zakresie cyberbezpieczeństwa poprzez praktyczne doświadczenie najpopularniejszych zagrożeń w bezpiecznym, kontrolowanym środowisku**.** Dostęp do platformy szkoleniowej musi wynosić minimum 30 dni dla 63 osób łącznie. Minimalne wymagania dotyczące platformy szkoleniowej:

Platforma szkoleniowa – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Wykonawca winien zapewnić dostęp do nowoczesnej platformy w formie strony www dostępnej w standardzie WCAG 2.1 – symulator zagrożeń internetowych. Symulator musi być narzędziem umożliwiającym użytkownikowi w bezpieczny sposób sprawdzenie oraz poznanie typowych zagrożeń czyhających na użytkowników w Internecie. Korzystanie z symulatora musi być całkowicie bezpieczne dla użytkownika końcowego (żadne z wpisywanych danych nie mogą być zapisywane i archiwizowane). W symulatorze konieczne jest zaimplementowanie min. 8 scenariuszy (zagrożeń) popularnych przestępstw internetowych, z którymi użytkownicy mogą się spotkać podczas codziennego korzystania z Internetu. Pierwsze cztery dotyczące tzw. Phishing'u w różnych odsłonach, (Phishing Clone, Phishing Spear, Phishing Spear Chat, Phishing Whaling) następny dotyczy oszustwa typu Pharming, dwa kolejne mają przedstawiać zasadę działania zagrożenia typu Malware, (Malware Post, Malware Email,) natomiast ostatni dotyczący certyfikatów SSL (Certificate Fraud Chat). Wykonawca zobowiązany jest przekazać zamawiającemu dostęp do platformy na minimum 30 dni od daty szkolenia, wraz z instrukcją obsługi. Wymagania szczegółowe dla platformy symulującej zagrożenia internetowe: a. Moduł podstron (fałszywych witryn) – moduł ten musi umożliwiać tworzenie różnego rodzaju fałszywych witryn nakłaniających użytkowników do pobierania zainfekowanych załączników, podawania danych wrażliwych i/lub dokonywania płatności internetowych. b. Moduł czatu – w module tym zaimplementowane mają być czat z botami, namawiającymi do zakupów różnych produktów powodując

	wyłudzenie danych osobowych, numerów kart kredytowych itp. W module tym zostaną zaimplementowane opracowane scenariusze c. Moduł e-mail – w module tym użytkownik musi mieć do przeglądnięcia kilka wiadomości e-mail przesłanych z różnych źródeł, wiadomości te będą zawierały linki bądź załączniki po kliknięciu których, zostanie uruchomiona akcja symulująca zachowanie się malware, np. blokada komputera (przeglądarki) na jakiś określony czas. Po kliknięciu załącznika „zainfekowanego" na ekranie powinna pojawić się informacja na temat, że twój komputer został zainfekowany, wykradliśmy twoje dane osobowe itd. Itp. W tym module należy również pokazać działanie tzw. szyfrującego wirusa, który po kliknięciu w załącznik szyfruje wszystkie pliki tekstowe, w tym przypadku symulator powinien pokazać przykład. d. Moduł edukacyjny – moduł musi zawierać szczegółowe informacje na temat występujących cyberprzestępstw. W szczególności powinien się skupić na phishingu, pharmingu oraz malware. Moduł ten powinien zawierać informacje na temat występowania oraz identyfikacji danego zagrożenia, sposobów zapobiegania, oraz informacji na temat, co użytkownik powinien w pierwszej kolejności zrobić, gdy zostanie już oszukany – czyli gdzie się zgłosić najpierw, jakie dane zabezpieczyć, zmienić hasła, czy zablokować karty płatnicze. Materiały edukacyjne powinny być przedstawione w formie plików PDF przedstawiających, na co zwrócić szczególną uwagę podczas korzystania z portali społecznościowych, różnego rodzaju czatów, różnego rodzaju serwisów internetowych oraz odbierania wiadomości e-mail. Moduł edukacyjny powinien być ściśle zintegrowany z pozostałymi modułami tj. Po przejściu każdego z opracowanych i zaimplementowanych w symulatorze scenariuszy powinna pojawić się informacja o tym jak i dlaczego użytkownik dał się oszukać i jakie to może mieć konsekwencje w późniejszym czasie. e. Moduł postów społecznościowych, zawierający możliwe ataki phishingowe lub pharmingowe, w module postów społecznościowych będą znajdować się zarówno „rzeczywiste" posty nie stanowiące zagrożenia jaki i posty z potencjalnym zagrożeniem.
Rozszerzone wsparcie serwisowe	System musi być objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez cały okres usługi. System musi być objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Przygotowanie do zdalnej konfiguracji. • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.

	Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego.