OPIS PRZEDMIOTU ZAMÓWIENIA

Zadanie nr 1

Szkolenie z zakresu cyberbezpieczeństwa i testów socjotechnicznych (Zadanie 2 - Obszar kompetencyjny / Lp. 3)

Zadanie polegające na przeprowadzeniu szkoleń z zakresu cyberbezpieczeństwa oraz przeprowadzeniu sprawdzających testów socjotechnicznych dla pracowników urzędu w okresie 18 miesięcy od podpisania umowy.

Opis przedmiotu zamówienia.

Zamawiający poszukuje dostawcy, który zaoferuje szkolenia z zakresu cyberbezpieczeństwa i budowania świadomości w zakresie bezpieczeństwa informacji.

Przedmiotem zamówienia jest kompleksowe kompleksowa szkolenie pracowników zgodnie z poniżej opisanym zakresem usługi.

Dostawca, który przeprowadzi szkolenia, musi spełniać następujące warunki:

1. posiadać co najmniej jeden z następujących certyfikatów:

- Certified Internal Auditor (CIA);
- Certified Information System Auditor (CISA);
- Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy o systemach oceny zgodności i nadzoru rynku;
- Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy o systemach oceny zgodności i nadzoru rynku;
- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems Control (CRISC);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified Information Systems Security Professional (CISSP);
- Systems Security Certified Practitioner (SSCP);
- Certified Reliability Professional;
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

2. posiadać udokumentowane doświadczenie w zakresie wdrożeń SZBI.
3. posiadać wdrożone polityki jakości i bezpieczeństwa zgodne z normami ISO 9001 oraz ISO/IEC 27001.

Zakres usługi:

- szkolenie personelu z zakresu cyberbezpieczeństwa oraz przeprowadzenie sprawdzających testów socjotechnicznych dla pracowników urzędu w okresie 24 miesięcy od podpisania umowy
- szkolenia stacjonarne w siedzibie Zamawiającego
- grupy maksymalnie 15 osobowe
- dwie grupy szkoleniowe
- szkolenie całodzienne dla grupy (6h szkoleniowych)
- 8 szkoleń w okresie trwania umowy (16 dni szkoleniowych)
- szkolenia zgodnie z poniższą listą tematów i zagadnień

1. Zagrożenia socjotechniczne: Analiza i Rozpoznawanie
   a) Omówienie różnych rodzajów zagrożeń socjotechnicznych.
   b) Szkolenie w zakresie identyfikacji manipulacji psychologicznych.
   c) Praktyczne przykłady ataków opartych na społeczeństwie.
   d) Dobre praktyki w Cyberbezpieczeństwie: Identyfikacja Zagrożeń.

2. Zapoznanie z aktualnymi trendami w dziedzinie cyberbezpieczeństwa.
   a) Omówienie skutecznych praktyk w identyfikacji potencjalnych zagrożeń.
   b) Analiza przypadków z życia codziennego.
   c) Cyberprzestępczość: Techniki i Narzędzia

3. Prezentacja najnowszych technik stosowanych przez cyberprzestępców.
   a) Analiza narzędzi używanych do przeprowadzania ataków.
   b) Studium przypadków znanego cyberprzestępczego działania.

4. Scenariusze Ataków: Przykłady i Analiza
   a) Modelowanie różnych scenariuszy ataków.
   b) Praktyczne przykłady ataków w oparciu o zamodelowane scenariusze.
   c) Dyskusja nad możliwymi środkami zaradczymi.
   d) Weryfikacja Procedur Zgłaszania Wiadomości E-mail.

5. Analiza obecnych procedur dotyczących zgłaszania podejrzanych wiadomości e-mail.
   a) Szkolenie pracowników w rozpoznawaniu potencjalnych zagrożeń w wiadomościach e-mail.
   b) Praktyczne ćwiczenia w zgłaszaniu podejrzanych sytuacji.

6. Bezpieczeństwo w Praktyce: Weryfikacja Zachowań Pracowników
   a) Monitorowanie i weryfikacja zachowań pracowników pod kątem bezpieczeństwa.
   b) Szkolenie w zakresie świadomości dotyczącej ryzyka.
   c) Praktyczne scenariusze i symulacje.

7. Ochrona Danych: Zasady i Procedury
   a) Omówienie zasad ochrony danych w kontekście urzędu gminy.
   b) Szkolenie w zakresie bezpiecznego przechowywania i przesyłania danych.
   c) Przykłady incydentów związanych z naruszeniem danych.

8. Bezpieczeństwo Fizyczne i Cyberbezpieczeństwo
   a) Integracja bezpieczeństwa fizycznego z cyberbezpieczeństwem.
   b) Szkolenie w zakresie ochrony infrastruktury fizycznej.
   c) Scenariusze łączące zagrożenia fizyczne i cyfrowe.

Zadanie nr 2

Wdrożenie wymagań ISO IEC 27001 (Zadanie 2 - Obszar kompetencyjny / Lp. 4)

Zadanie polegające na kompleksowym wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) opartego na normie ISO/IEC 27001.

Opis przedmiotu zamówienia.

Zamawiający poszukuje dostawcy, który zaoferuje kompleksowe wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) opartego na normie ISO/IEC 27001 oraz przeprowadzi szkolenia z zakresu cyberbezpieczeństwa i budowania świadomości w zakresie bezpieczeństwa informacji. Przedmiotem zamówienia jest kompleksowe wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z normą ISO/IEC 27001.

Dostawca, który przeprowadzi wdrożenie SZBI, musi spełniać następujące warunki:

1. Posiadać w swoich zasobach osobowych pracowników legitymujących się jednym z następujących certyfikatów:
   - Certified Internal Auditor (CIA);
   - Certified Information System Auditor (CISA);
   - Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy o systemach oceny zgodności i nadzoru rynku;
   - Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy o systemach oceny zgodności i nadzoru rynku;
   - Certified Information Security Manager (CISM);
   - Certified in Risk and Information Systems Control (CRISC);
   - Certified in the Governance of Enterprise IT (CGEIT);
   - Certified Information Systems Security Professional (CISSP);
   - Systems Security Certified Practitioner (SSCP);
   - Certified Reliability Professional;
   - Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

1. Posiadać udokumentowane doświadczenie w zakresie wdrożeń SZBI.
2. Posiadać wdrożone polityki jakości i bezpieczeństwa zgodne z normami ISO 9001 oraz ISO/IEC 27001.

Zakres usługi:

1. analiza ryzyka i oceny zgodności z wymaganiami normy ISO/IEC 27001.
2. projektowanie i implementacja odpowiednich procedur, polityk i kontroli bezpieczeństwa.
3. opracowanie dokumentacji niezbędnej do uzyskania certyfikacji zgodności z normą ISO/IEC 27001.
4. szkolenie personelu z zakresu obsługi SZBI oraz przepisów dotyczących bezpieczeństwa informacji.