Załącznik nr 1 przedmiot zamówienia

Opis przedmiotu zamówienia
na organizację szkoleń w ramach projektu pn. „Podniesienie poziomu cyberbezpieczeństwa w Urzędzie Miejskim w Koninie" realizowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027

Określenie przedmiotu zamówienia:

Przedmiotem zamówienia jest usługa polegająca na organizacji szkoleń w ramach projektu pn. „Podniesienie poziomu cyberbezpieczeństwa w Urzędzie Miejskim w Koninie" realizowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027

I. SZKOLENIA DLA PRACOWNIKÓW URZĘDU MIEJSKIEGO W KONINIE

Szkolenie w wersji elektronicznej

1. **Przedmiot zamówienia:** Szkolenie w wersji elektronicznej (e-learning) z zakresu bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego. Szkolenia dedykowane dla pracowników biurowych (nietechnicznych) pracujących z komputerami i przetwarzających różnego rodzaju informacje o różnym poziomie poufności. Szkolenia muszą być w formie gotowego produktu dostarczanego Zamawiającemu bezzwłocznie po złożeniu zamówienia / podpisaniu umowy. Zamawiający musi mieć możliwość swobodnego wykorzystania szkoleń bez ograniczeń czasowych oraz liczby odbiorców.
2. **Forma e-learning:** Szkolenie musi być w postaci oddzielnych lekcji dla każdej z kategorii z niżej opisanego zakresu. Jedna lekcja szkolenia powinna zawierać minimum 30 slajdów. Czas jednej lekcji (tematu) powinien oscylować w granicach 20-30 min. Lekcje powinny być multimedialne z wykorzystaniem między innymi scenek rodzajowych z możliwością odtworzenia w postaci dźwiękowej z użyciem lektora. Nie mogą to być same zdjęcia, definicje lub zagadnienia opisane w formie tekstowej i odtwarzane w postaci dźwiękowej. Podczas lekcji powinna być na bieżąco weryfikowana wiedza (uwaga) użytkownika poprzez np. ćwiczenia sprawdzające.
3. **Zakres tematyczny dla bezpieczeństwa teleinformatycznego:** Szkolenie musi posiadać oddzielne lekcje dla co najmniej następujących zagadnień:
   1. Czym jest bezpieczeństwo informacji;
   2. Aspekty prawne związane z bezpieczeństwem informacji;
   3. Czym jest phishing?

4. Zasady korzystania z Internetu;
5. Zasady korzystania z portali społecznościowych;
6. Zasady korzystania z poczty elektronicznej i zagrożenia z tym związane;
7. Zasady korzystania z bezpiecznych haseł;
8. Zagrożenia i sposoby zabezpieczania sprzętu mobilnego;
9. Metody pozyskiwania informacji (socjotechnika);
10. Bezpieczeństwo w zakresie płatności elektronicznych;
11. Bezpieczeństwo fizyczne w zakresie zabezpieczania pomieszczeń, dokumentacji, sprzętu IT;
12. Czym jest ransomware i jak wygląda w praktyce;
13. Jak bezpiecznie korzystać z menedżera haseł w praktyce;
14. Techniki stosowane przez cyberprzestępców;
15. Uważaj by nie zostać „mułem finansowym";
16. Bezprzewodowe życie;
17. Praca zdalna - jak zrealizować ją bezpiecznie?
18. Vishing... co to jest?
19. Phishing – stare problemy, nowe sposoby. Przykłady aktualnych cyberataków i sposoby ochrony przed nimi;
20. Jak cyberprzestępcy kradną dane przez telefon;
21. Fake news i dezinformacja;
22. Jak zapewnić ciągłość działania;
23. Cloud. O co chodzi w chmurach obliczeniowych?
24. AI - wielka szansa czy olbrzymie zagrożenie?
25. NIS 2 - nowa dyrektywa - nowy poziom bezpieczeństwa w UE;
26. Test z imiennym certyfikatem ukończenia kursu.

4. Forma szkolenia:

a. Szkolenie musi posiadać atrakcyjną formę przekazu materiału, zachęcającą osoby uczące się do aktywnego odbywania szkolenia. Zamawiający wymaga atrakcyjnej formy przekazu materiału szkolenia. Atrakcyjna forma to m.in. grafika oparta na scenkach, postaciach, dialogach, przykładach, ćwiczeniach, testach sprawdzających wiedzę oraz dźwięk – głos lektorów indywidualny dla każdej z postaci występujących w szkoleniu.

b. Szkolenie musi posiadać interaktywną formę, zwiększającą zaangażowanie osób uczących się. Szkolenie musi zostać wyposażone w elementy interakcji (np. kliknięcia, ćwiczenia), tak aby uczestnik był aktywny podczas szkolenia i nie miał możliwości

zaliczenia szkolenia w sposób bierny tj. poprzez samoczynne odtworzenia filmu/ szkolenia.

c. Lekcje szkolenia muszą kłaść duży nacisk na umiejętności praktyczne, nie tylko teorię bezpieczeństwa IT. W celu zwiększenia praktycznej przydatności szkolenia musi ono zostać opracowane tak, aby zajęcia kładły większy nacisk na umiejętności praktyczne użytkowników komputerów (np. wykrywanie sytuacji zagrożenia w trakcie korzystania z serwisów społecznościowych, właściwe postępowanie w razie incydentu) niż samą teorię bezpieczeństwa IT.

d. Cały materiał szkolenia musi być dostępny w języku polskim i przedstawiony w sposób zrozumiały przez osoby nietechniczne.

e. Szkolenie musi posiadać wysoką jakość merytoryczną przygotowanego scenariusza. Scenariusz szkolenia musi zostać opracowany we współpracy z ekspertem bezpieczeństwa IT posiadającym certyfikat Lead Auditor 27001. Certyfikat oferent musi przedstawić zamawiającemu łączenie z oświadczeniem audytora o poprawności merytorycznej przygotowanych materiałów.

5. **Wymagania techniczne:** Szkolenie w wersji elektronicznej musi być zgodne ze standardem umożliwiającym prezentację na **platformie MOODLE w wersji 4.0 lub wyższej**. Szkolenie powinno być dostarczone w technologii **SCORM 2004**. Szkolenia powinny być podzielone tematycznie w taki sposób, aby można było operować (zarządzać dostępnością, harmonogramem, itp.) poszczególnymi tematami z osobna. Zamawiający wymaga wsparcia technicznego w procesie wdrażania e-szkoleń na platformie MOODLE u zamawiającego.

6. Warunki licencji: Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na szkolenie. Szacunkowa liczba osób do przeszkolenia wynosi 250 Pracowników, licencja zostanie udzielona na nieograniczoną liczbę pracowników z możliwością wykorzystania szkolenia w podległych jednostkach organizacyjnych Zamawiającego.

7. Wykonawca zobowiązuje się do prawidłowego wykonania wszystkich prac związanych z realizacją przedmiotu zamówienia.

8. **Termin dostawy: 30 dni od daty zawarcia umowy.**

II. SPECJALISTYCZNE SZKOLENIA DLA KADRY ZARZĄDZAJĄCEJ

Szkolenia dla kadry zarządzającej w Urzędzie Miejskim w Koninie (prezydenci, skarbnicy oraz sekretarz) w zakresie bezpieczeństwa informacji mają obejmować odpowiednio:

a) Szkolenie z zakresu bezpieczeństwa informacji zostanie przeprowadzone w formie stacjonarnej w siedzibie Zamawiającego dla 7 uczestników w terminie do 30.11.2025 r.

b) Jednostką czasową szkolenia jest 1 godzina szkoleniowa (45 minut).

c) Szkolenie będzie trwało minimum 6 godzin szkoleniowych.

d) Szkolenie będzie odbywać się w czasie godzin pracy Zamawiającego, tj. min. 6 godzin między 7.30-15.30, po wcześniejszych ustaleniach z Zamawiającym.

e) Szkolenie będzie prowadzone w języku polskim.

f) Szkolenie prowadzone będzie na podstawie zaakceptowanego przez Zamawiającego harmonogramu zawierającego zakres merytoryczny i terminy, dostarczonego przez Wykonawcę Zamawiającemu przed podpisaniem umowy. Brak uzgodnienia harmonogramu stanowi podstawę odstąpienia od podpisania umowy.

Tematyka szkolenia będzie dotyczyła w szczególności następujących zagadnień z zakresu bezpieczeństwa informacji:

1. Wprowadzenie do tematyki związanej z ochroną przed cyberzagrożeniami. Bezpieczeństwo informacji w świetle rozwijających się technologii.
2. System zarządzania bezpieczeństwem informacji wynikających z ISO/IEC 27001, a cyberbezpieczeństwo. Kluczowe obszary.
3. Przegląd zagrożeń dla bezpieczeństwa informacji przetwarzanych formą tradycyjną oraz elektroniczną.
4. Źródła zagrożeń związanych z bezpieczeństwem informacji oraz ich klasyfikacja w oparciu o możliwe zdarzenia i straty dla organizacji.
5. Zarządzanie ryzykiem, jako kluczowy element ochrony. Podejście praktyczne.
6. Najczęstsze praktyki i sposoby wyłudzania, oszustw lub kradzieży informacji z organizacji:
    - wykradanie danych,
    - phishing i zaawansowane techniki wykorzystywane przez cyberprzestępców,
    - ataki socjotechniczne,
    - malware,
    - kontrola dostepu,
    - działania pracowników wewnętrznych na szkodę organizacji,
    - techniki manipulacji,
    - biały wywiad,
    - ataki destrukcyjne.

7. Case study: atak ukierunkowany (APT) na osoby zarządzające i zbudowanie roadmapy ataku.
8. Case study: Jak zwykły spam może prowadzić do poważnych konsekwencji. Spojrzenie okiem biegłego sądowego z zakresu przestępstw przy pomocy systemów IT.
9. Zarządzanie aktywami informacyjnym.
10. Najlepsze praktyki w zakresie cyberbezpieczeństwa stosowane na świecie:
    - Zarządzanie dostępem do sieci i systemów IT.
    - Korzystanie z sieci bezprzewodowych w pracy i w domu.
    - Bezpieczne korzystanie z urządzeń mobilnych (telefony, tablety, laptopy)
    - Ataki przez telefon
    - Bezpieczne przechowywanie i usuwanie danych (na komputerze i na pendrive)
    - Bezpieczna praca z przeglądarką internetową
    - Problem aktualnego oprogramowania i kopii zapasowych
    - Praca zdalna - ocena z perspektywy audytora. Ryzyka, rekomendacje.
    - Zarządzanie hasłami;
    - Wdrażania silnych mechanizmów ochrony przed kradzieżą sprzętu i tożsamości oraz nieautoryzowanym dostępem do zasobów organizacji.
    - Dostęp uprzywilejowany,
    - Polityka czystego biurka i czystego ekranu,
    - Korzystanie z urządzeń końcowych nagrywających dźwięk i obraz.
11. Case study: Mamy incydent i co teraz. Tworzenie schematu postępowania zarządzania incydentami.
12. Rola pracownika w doskonaleniu ochrony oraz postępowanie z najczęstszymi incydentami związanymi z bezpieczeństwem informacji.
13. Wymagania trenera:

Osoba prowadząca szkolenie winna:

1) posiadać i przedstawić ważne na dzień realizacji szkolenia certyfikaty:
    - Audytor wiodący ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności lub równoważny
    - Audytor wiodący ISO/IEC 27701 - System Zarządzania Informacjami o Prywatności lub równoważny

- Audytor wiodący ISO/IEC 27018 – Kodeks postępowania w zakresie ochrony informacji umożliwiających identyfikację osoby w chmurach publicznych działających jako podmioty przetwarzające PII lub równoważny.

III. SPECJALISTYCZNE SZKOLENIA DLA INFORMATYKÓW

1. **Przedmiot zamówienia:**
   Usługa na szkolenie stacjonarne w zakresie cyberbezpieczeństwa oraz bezpieczeństwa informacji. Szkolenie dedykowane dla administratorów IT Urzędu Miejskiego w Koninie

2. **Forma szkolenia:**
   a) Szkolenia zostaną przeprowadzone w formie stacjonarnej w siedzibie Zamawiającego (ul. Plac Wolności 1) dla 8 uczestników.
   b) Jednostką czasową szkolenia jest 1 godzina szkoleniowa (45 minut).
   c) Szkolenia będą trwały minimum 16 godzin szkoleniowych .
   d) Szkolenia będą odbywać się w dni robocze w godzinach 14.00 – 18.00 w terminie uzgodnionym z Zamawiającym.
   e) Szkolenia będą prowadzone w języku polskim.
   f) Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego harmonogramu zawierającego zakres merytoryczny i terminy, dostarczonego przez Wykonawcę Zamawiającemu przed podpisaniem umowy.
   Brak uzgodnienia harmonogramu stanowi podstawę odstąpienia od podpisania umowy.

3. **Zakres tematyczny szkolenia:**
   a) Wprowadzenie do tematyki związanej z ochroną przed cyberzagrożeniami. Bezpieczeństwo informacji w świetle rozwijających się technologii,
   b) System zarządzania bezpieczeństwem informacji wynikających z ISO/IEC 27001 lub równoważnych, a cyberbezpieczeństwo. Kluczowe obszary.
   c) Przegląd zagrożeń dla bezpieczeństwa informacji przetwarzanych formą tradycyjną oraz elektroniczną.
   d) Źródła zagrożeń związanych z bezpieczeństwem informacji oraz ich klasyfikacja w oparciu o możliwe zdarzenia i straty dla organizacji.
   e) Zarządzanie ryzykiem, jako kluczowy element ochrony. Podejście praktyczne.
   f) Najczęstsze praktyki i sposoby wyłudzania, oszustw lub kradzieży informacji z organizacji:
      - wykradanie danych,
      - phishing i zaawansowane techniki wykorzystywane przez cyberprzestępców,

- ataki socjotechniczne,
- malware,
- kontrola dostępu,
- działania pracowników wewnętrznych na szkodę organizacji,
- techniki manipulacji,
- biały wywiad,
- ataki destrukcyjne.

g) Case study: atak ukierunkowany (APT) na osoby mające dostęp do systemów i danych finansowych.

h) Normy, standardy, wytyczne wspomagające zarządzanie systemami IT

- ISO 2700x,
- Krajowe Ramy Interoperacyjności,
- RODO
- Ustawa krajowy system cyberbezpieczeństwa,

i) System Zarządzania bezpieczeństwem informacji,

j) Najlepsze praktyki zabezpieczania systemów informacyjnych:

- infrastruktura IT i ochrona danych w data center/serwerowni,
- podstawowa dokumentacja i wdrożone polityki bezpieczeństwa,
- organizacji bezpieczeństwa informacji,
- zarządzania aktywami IT,
- kontrola dostępu (sieć, systemy, aplikacje, urządzenia),
- bezpieczeństwo sprzętu,
- zarządzania systemami i sieciami,
- procedury eksploatacyjne i zakresy odpowiedzialności,
- zarządzanie usługami dostarczanymi przez strony trzecie,
- planowanie i odbiór systemów,
- ochrona przed kodem złośliwym,
- kopie zapasowe,
- zarządzanie bezpieczeństwem sieci,
- obsługa nośników,
- monitorowanie,
- bezpieczne sposoby wymiany informacji,
- przetwarzanie mobilne i praca na odległość,
- zarządzanie bezpieczeństwem danych przetwarzanych w modelu cloud,
- pozyskiwania i rozwoju systemów informatycznych,
- zarządzania relacjami z dostawcami,
- zarządzania incydentami w systemach IT,

- zarządzania ciągłością działania,
- compliance.

h) Najczęściej zidentyfikowane w czasie audytów czy kontroli incydenty, słabości, naruszenia i przestępstwa omówione z perspektywy audytora wiodącego i biegłego sądowego.

4. Wymagania trenera:

Osoba prowadząca szkolenie winna:

1) posiadać i przedstawić ważne na dzień realizacji szkolenia certyfikaty:

- Audytor wiodący ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności lub równoważny
- Audytor wiodący ISO/IEC 27701 - System Zarządzania Informacjami o Prywatności lub równoważny
- Audytor wiodący ISO/IEC 27018 – Kodeks postępowania w zakresie ochrony informacji umożliwiających identyfikację osoby w chmurach publicznych działających jako podmioty przetwarzające PII lub równoważny

5. Termin realizacji:

60 dni od daty zawarcia umowy.

IV. FortiGate Administrator

Ilość osób – 1

Plan szkolenia:

- System and Network Settings
- Firewall Policies and NAT
- Routing
- Firewall Authentication
- Fortinet Single Sign-On (FSSO)
- Certificate Operations
- Antivirus
- Web Filtering
- Intrusion Prevention and Application Control
- SSL VPN

- IPsec VPN
- SD-WAN Configuration and Monitoring
- Security Fabric
- High Availability
- Diagnostics and Troubleshooting

Forma szkolenia:
Czas trwania: 4 dni
- online
Wymagania:

- Kurs kończy się wydanym imiennym certyfikatem wystawionym przez FORTINET lub równoważnym.

- Trener – Certyfikowany Trener Fortinet (FCT).

Z uwagi na szczególny zakres i charakter szkolenia, dotyczącego posiadanego przez Zamawiającego urządzenia, wymaga się, aby Trener posiadał certyfikację szkoleniową producenta tego urządzenia lub podmiotu działającego w ramach jego autoryzacji. Dopuszcza się równoważne certyfikacje, pod warunkiem, iż zostaną one uwierzytelnione (potwierdzone) przez producenta urządzenia FortiGate.

Ww dokumenty wykonawca zobowiązany jest przedłożyć przed podpisaniem umowy. Ich niedostarczenie lub dostarczenie dokumentów nieodpowiadających powyższym wymogom stanowi podstawę do odstąpienia od podpisania umowy.

V . Network Security Support Engineer

Ilość osób - 1

Plan szkolenia:

- Troubleshooting Concepts
- System Resources
- Sessions, Traffic Flow, and Networking
- Security Fabric
- Firewall Authentication
- FSSO

- Security Profiles
- High Availability
- IPsec
- IPsec-IKEv2
- BGP
- OSPF

Forma szkolenia :
- online lub stacjonarnie w ośrodku szkoleniowym
Czas trwania: 3 dni

Wymagania :

- Kurs kończy się wydanym imiennym certyfikatem wystawionym przez FORTINET lub równoważnym.

- Trener – Certyfikowany Trener Fortinet (FCT) .

Z uwagi na szczególny zakres i charakter szkolenia, dotyczącego posiadanego przez Zamawiającego urządzenia, wymaga się, aby Trener posiadał certyfikację szkoleniową producenta tego urządzenia lub podmiotu działającego w ramach jego autoryzacji. Dopuszcza się równoważne certyfikacje, pod warunkiem, iż zostaną one uwierzytelnione (potwierdzone) przez producenta urządzenia FortiGate.

Ww dokumenty wykonawca zobowiązany jest przedłożyć przed podpisaniem umowy. Ich niedostarczenie lub dostarczenie dokumentów nieodpowiadających powyższym wymogom stanowi podstawę do odstąpienia od podpisania umowy.

VI. Implementing and Administering Cisco Solutions v2.1

Ilość osób - 1

Plan szkolenia:

1. Definicja sieci komputerowej
2. Komunikacja w sieci
3. System operacyjny IOS
4. Wprowadzenie do sieci lokalnych
5. Warstwa łącza w modelu TCP/IP

6. Praca z przełącznikami
7. Wprowadzenie do warstwy Internetu modelu TCP/IP, adresacja IPv4 i podsieci
8. Warstwa transportu i aplikacji modelu TCP/IP
9. Routing w sieciach
10. Konfiguracja routera Cisco
11. Proces dostarczania pakietów
12. Znajdowanie błędów w prostych sieciach
13. Routing pomiędzy sieciami VLAN
14. Wprowadzenie do protokołu OSPF
15. Budowa nadmiarowych sieci przełączanych
16. Agregacja łączy za pomocą EtherChannel
17. Listy kontroli dostępu
18. Łączność z siecią Internet
19. Wprowadzenie sztucznej inteligencji i uczenia maszynowego do operacji sieciowych
20. Monitoring systemu
21. Zarządzanie urządzeniami Cisco
22. Zabezpieczanie dostępu administracyjnego
23. Utwardzanie urządzeń sieciowych

Forma szkolenia :
- online lub stacjonarnie w ośrodku szkoleniowym
Czas trwania: 5 dni

Wymagania :

- Kurs kończy się wydanym imiennym certyfikatem wystawionym przez CISCO lub równoważnym.

- Wykonawca musi posiadać autoryzację Cisco.

Z uwagi na szczególny zakres i charakter szkolenia, dotyczącego posiadanego przez Zamawiającego urządzenia i oprogramowania, wymaga się, aby Trener posiadał certyfikację szkoleniową producenta tego urządzenia / oprogramowania lub podmiotu działającego w ramach jego autoryzacji. Dopuszcza się równoważne certyfikacje, pod warunkiem, iż zostaną one uwierzytelnione (potwierdzone) przez producenta urządzenia / oprogramowania Cisco.

Ww dokumenty wykonawca zobowiązany jest przedłożyć przed podpisaniem umowy. Ich niedostarczenie lub dostarczenie dokumentów nieodpowiadających powyższym wymogom stanowi podstawę do odstąpienia od podpisania umowy.

VII . Managing Windows Server 2022

Ilość osób - 8

Program szkolenia

1. Wprowadzenie do Windows Server 2022
2. Zarządzanie Windows Server 2022
3. Wprowadzenie do Active Directory
4. Wprowadzenie do obiektów zasad grupy (GPO)
5. Wprowadzenie do wykorzystania certyfikatów w środowisku Windows Server 2022
6. Wprowadzenie do usług sieciowych
7. Domain Name System (DNS)
8. Dynamic Host Configuration Protocol (DHCP)
9. Dostęp zdalny w środowisku Windows Server 2022
10. Wprowadzenie do Remote Desktop Services (RDS)
11. Zarządzanie systemem plików i przestrzenią dyskową
12. Monitorowanie pracy serwera
13. Odzyskiwanie po awarii
14. Wprowadzenie do wirtualizacji systemów operacyjnych (Hyper-V)

Forma szkolenia :
- online

Wymagania :

- Kurs kończy się wydanym imiennym certyfikatem.

Termin realizacji przedmiotu zamówienia.

Termin wykonania przedmiotu zamówienia– od dnia podpisania umowy do 30-11-2025r.