

1. Przedmiotem zamówienia jest **przeprowadzenie rozbudowanego szkolenia w zakresie cyberbezpieczeństwa dedykowanego administratorom systemów informatycznych w jednostkach samorządu terytorialnego (JST)**. Szkolenie ma na celu podniesienie poziomu wiedzy i umiejętności w zakresie ochrony systemów dziedzinowych oraz eUsług świadczonych przez JST w kontekście wdrażania i utrzymania polityk bezpieczeństwa informacji oraz zarządzania bezpieczeństwem informacji.

Zakres szkolenia:

1. **Podstawy cyberbezpieczeństwa w JST:**
 - o Przegląd zagrożeń w cyberprzestrzeni: ataki ransomware, phishing, spoofing, ataki na eUsługi.
 - o Rola administratora w ochronie systemów JST.
2. **Tworzenie i wdrażanie polityk bezpieczeństwa informacji:**
 - o Opracowanie polityk zgodnych z KRI, RODO i KSC.
 - o Tworzenie strategii ochrony danych oraz procedur działania w przypadku naruszeń bezpieczeństwa.
3. **Ochrona systemów dziedzinowych i eUsług:**
 - o Techniki wzmacniania zabezpieczeń systemów dziedzinowych (np. systemy ERP, CRM, systemy rejestrów).
 - o Bezpieczne udostępnianie eUsług dla obywateli z zachowaniem integralności i poufności danych.
4. **Analiza ryzyka i zarządzanie incydentami:**
 - o Metody identyfikacji zagrożeń i oceny ryzyka.
 - o Zarządzanie incydentami: od detekcji po reakcję i usuwanie skutków.
 - o Planowanie i utrzymanie ciągłości działania w sytuacjach kryzysowych.
5. **Nowoczesne narzędzia i technologie:**
 - o Wykorzystanie zaawansowanych rozwiązań do ochrony danych (np. szyfrowanie, uwierzytelnianie wieloskładnikowe).
 - o Monitoring systemów i analiza logów bezpieczeństwa.
 - o Automatyzacja zadań w ochronie systemów JST.

Efekty szkolenia:

Po ukończeniu szkolenia uczestnicy zdobędą:

- Umiejętności wdrażania skutecznych polityk bezpieczeństwa w JST.

- Praktyczne zdolności w zabezpieczaniu systemów dziedzinowych i eUsług przed cyberatakami.
- Wiedzę na temat zarządzania incydentami i planowania działań zapewniających ciągłość funkcjonowania JST.

Cel: Wyposażenie administratorów w narzędzia i kompetencje niezbędne do ochrony danych i systemów JST w dynamicznie zmieniającym się środowisku zagrożeń cyfrowych, przy jednoczesnym podnoszeniu standardów bezpieczeństwa w zakresie świadczonych eUsług.

2. Przedmiotem zamówienia jest **przeprowadzenie kompleksowego szkolenia dla pracowników jednostek samorządu terytorialnego (JST)**, mającego na celu rozwój kompetencji cyfrowych oraz podniesienie poziomu bezpieczeństwa systemów informatycznych w JST. Szkolenie skierowane jest do osób odpowiedzialnych za codzienną obsługę systemów IT oraz przetwarzanie danych, z naciskiem na praktyczne umiejętności wykorzystywane w ich codziennej pracy.

Zakres szkolenia:

1. Rozwój kompetencji cyfrowych

- Podstawy efektywnej obsługi systemów IT: zarządzanie dokumentacją elektroniczną, praca w chmurze, podstawy korzystania z e-usług administracji publicznej.
- Narzędzia biurowe: zaawansowane funkcje pakietów biurowych, automatyzacja zadań, wykorzystanie aplikacji wspierających pracę zespołową (np. Microsoft Teams).
- Cyfrowa komunikacja w JST: narzędzia do zarządzania pocztą elektroniczną, ochrona przed oszustwami typu phishing.

2. Podstawy cyberbezpieczeństwa dla pracowników JST

- Świadomość cyberzagrożeń: rozpoznawanie prób oszustw, ataków phishingowych, ransomware i malware.
- Cyberhigiena: bezpieczne hasła, aktualizacje systemów, ochrona urządzeń mobilnych.
- Zasady bezpiecznego korzystania z sieci: zarządzanie dostępem, unikanie ryzykownych stron i załączników.
- Zabezpieczanie danych: tworzenie i przechowywanie kopii zapasowych, szyfrowanie plików i komunikacji.

3. Bezpieczeństwo systemów informatycznych w JST

- Ochrona systemów dziedzinowych: podstawowe zasady obsługi i ochrony najczęściej używanych w JST systemów (np. systemów księgowych, rejestrów mieszkańców).
- Podstawy zarządzania dostępem do systemów: przydzielanie ról, kontrola logowań, zapobieganie wyciekom danych.
- Procedury w sytuacjach kryzysowych: reagowanie na naruszenia bezpieczeństwa i współpraca z zespołem IT.

- Ochrona systemów e-usług świadczonych przez JST: zabezpieczenie portali dla obywateli.

5. Zagadnienia prawne i regulacyjne

- RODO i ochrona danych osobowych w JST: odpowiedzialność pracowników w zakresie przetwarzania danych.
- Krajowe Ramy Interoperacyjności (KRI): kluczowe wymogi dotyczące bezpieczeństwa systemów IT w administracji publicznej.
- Krajowy System Cyberbezpieczeństwa (KSC): obowiązki JST wynikające z ustawy.

Efekty szkolenia:

1. Pracownicy JST podniosą swoje kompetencje cyfrowe, zwiększając efektywność pracy z systemami IT.
2. Zyskają umiejętności umożliwiające identyfikację i zapobieganie zagrożeniom cyfrowym.
3. Będą w stanie lepiej zabezpieczyć systemy JST, e-usługi i dane obywateli przed cyberatakami.
4. Poznają obowiązujące przepisy i standardy bezpieczeństwa, co ułatwi wdrażanie zgodnych z prawem procedur.

Cel szkolenia:

Stworzenie w JST zespołu kompetentnych i świadomych cyfrowo pracowników, którzy nie tylko efektywnie obsługują systemy IT, ale również aktywnie wspierają bezpieczeństwo informacji, chroniąc dane obywateli i kluczowe systemy administracji publicznej.

