



Opis przedmiotu zamówienia

Cele szkolenia: Zrozumienie roli każdego pracownika w systemie ochrony informacji, zapoznanie z wymogami prawnymi oraz nauka właściwego reagowania na zagrożenia. Podniesienie świadomości pracowników w zakresie cyberbezpieczeństwa. Zwiększenie wiedzy kadry IT z zakresu użycia profesjonalnych narzędzi do wykonywania kopii zapasowych.

Grupa docelowa: Pracownicy jednostek Gminy Nidzica tj.: Urzędu Miejskiego w Nidzicy (UMN), Centrum Usług Wspólnych (CUW), Miejskiego Ośrodka Pomocy Społecznej (MOPS), Miejskiego Ośrodka Sportu i Rekreacji (MOSiR) oraz 8 jednostek oświatowych. Szacowana liczba uczestników szkolenia 153 osoby, w tym szacuje się: 124 K i 29 M. Zamawiający wymaga, aby szkolenie przeprowadzone zostało z podziałem na grupy szkoleniowe nie większe niż 35 osób. Kompetencyjnie grupy mają być podzielone na:

- kadra zarządzająca (35 pracowników – 2 grupy szkoleniowe, min. 3 godz. Szk.I i Szk.III),
- kadra IT (5 pracowników – indywidualny dobór terminu z Zamawiającym, min. 32 godz. Szk.II),
- pozostali pracownicy jednostek (113 pracowników – 4 grupy szkoleniowe, min. 3 godz. Szk.I i Szk.III)

Wykonawca uzgodni z Zamawiającym szczegółowy zakres, formę i harmonogram prowadzonych szkoleń.

Minimalny zakres prowadzonych szkoleń:

I. Szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST z ankietą weryfikującą wiedzę – min. 3 godz., obejmujące:

1. Normy prawne i kluczowe role z zakresu bezpieczeństwa informacji.
2. Kluczowe definicje z zakresu bezpieczeństwa informacji (ISO/IEC 27001)
 - a. Informacja i jej rodzaje (papierowa, elektroniczna, ustna).
 - b. Dane osobowe, identyfikatory, szczególne kategorie danych.
 - c. Bezpieczeństwo: poufność, integralność, dostępność; rozliczalność i niezaprzeczalność.
 - d. Incydent bezpieczeństwa
 - e. Uwierzytelnianie i autoryzacja.
 - f. Ryzyko jako zdarzenie mające wpływ na osiągnięcie celów organizacji, metody szacowania i oceny.
 - g. System Zarządzania Bezpieczeństwem Informacji w ujęciu procesowym.
3. Role i zadania osób odpowiedzialnych za bezpieczeństwo informacji:
 - a. Administrator danych (Kierownik jednostki).



Cyberbezpieczny Samorząd

- b. Koordynator ds. cyberbezpieczeństwa.
 - c. Koordynator ds. bezpieczeństwa fizycznego.
 - d. Administrator Systemów Informatycznych (ASI).
 - e. Inspektor Ochrony Danych (IOD).
 - f. Kierownicy, w tym zarządzający jednostkami organizacyjnymi.
 - g. Pracownicy.
4. Procedura zgłoszenie incydentu (system), dla pracowników JST i podległych jednostek organizacyjnych.
5. Analiza ryzyka *dla kadry zarządzającej (warsztaty)*:
 - a. Wprowadzenie do analizy ryzyka oraz cel jej przeprowadzenia.
 - b. Identyfikacja zagrożeń i podatności, definicja incydentu w rozumieniu ISO/IEC 27001.
 - c. Ocena ryzyka jako fundament SZBI.
 - d. Zarządzanie ryzykiem, w tym zgłoszenie incydentu, reakcja oraz jego dokumentowanie.
 - e. Przeprowadzenie analizy ryzyka – forma warsztatów opartych na narzędziach informatycznych.
6. Tworzenie planów minimalizacji ryzyk *dla kadry zarządzającej (warsztaty)*.

II. Szkolenie specjalistyczne dla kadry IT w zakresie stosowanych środków bezpieczeństwa w ramach projektu grantowego, obejmujące:

1. Stosowanie i aktualizacja procedury zarządzania kopiami zapasowymi danych:
 - a. Proces zarządzania kopiami zapasowymi;
 - b. Procedura wykonywania kopii zapasowych;
 - c. Procedura testowania kopii zapasowych;
 - d. Procedura odzyskiwania danych i systemów informatycznych z kopii zapasowych.
2. Certyfikowane szkolenie akredytowane z narzędzi do wykonywania kopii zapasowych Veeam dla Kadry IT (min. 32 godz. szkoleniowych – min. 4 dni) zapewniające:
 - a. Wyjaśnienie roli każdego z podstawowych komponentów oprogramowania do kopii zapasowych.
 - b. Skonfigurowanie oprogramowania do kopii i zarządzanie nim.
 - c. Skonfigurowanie zadań tworzenia kopii zapasowych w oparciu o scenariusze.
 - d. Ochrona serwerów fizycznych za pomocą agentów.
 - e. Konfigurowanie zadań tworzenia kopii zapasowych danych nieustrukturyzowanych (udostępnienia NAS/SMB itp.)
 - f. Przedstawienie możliwości w zakresie replikacji danych.





Cyberbezpieczny Samorząd

- g. Przedstawienie odpowiednich przypadków użycia dla funkcji wykonywania kopii zapasowych, replikacji i ciągłej ochrony danych.
- h. Przedstawienie możliwości w zakresie odzyskiwania kopii zapasowych oraz funkcji niezmiennych repozytoriów.
- i. Przedstawienie koncepcji bezpieczeństwa i sposobów ich wdrażania.
- j. Konfiguracja wykrywania i usuwania złośliwego oprogramowania.
- k. Przedstawienie możliwości odzyskiwania danych z kopii zapasowych maszyn wirtualnych, agentów i aplikacji w konkretnych scenariuszach.
- l. Przedstawienie funkcji monitorowania, raportowania i alertowania.
- m. Przedstawienie podstawowych procedur rozwiązywania problemów i współpracy z pomocą techniczną.

III. Szkolenie weryfikujące świadomość zagrożeń i reakcji personelu (min. 3 godz.) połączone z prowokacją i testem w UM, CUW, MOPS:

- a. Socjotechnika i Phishing: Rozpoznawanie podejrzanych wiadomości e-mail, linków oraz technik manipulacji.
 - phishing i spear phishing
 - ransomware
 - złośliwe załączniki i linki
 - socjotechnika (telefon, e-mail, „na policjanta”, „na przełożonego”)
 - analiza prawdziwych maili phishingowych
 - identyfikacja podejrzanych elementów (adres, link, styl wiadomości)
 - Bezpieczna praca z pocztą i Internetem
 - zasady otwierania załączników
 - sprawdzanie linków
 - korzystanie z przeglądarki i stron WWW
 - zagrożenia związane z pobieraniem plików
 - „czy kliknąłbyś?” – analiza przykładów
 - rozpoznawanie fałszywych stron (np. logowania)
- b. Bezpieczeństwo haseł i uwierzytelnianie: Zasady tworzenia silnych haseł oraz stosowanie uwierzytelniania wieloskładnikowego (MFA).
 - jak tworzyć silne hasła
 - menedżery haseł
 - uwierzytelnianie wieloskładnikowe (MFA)
 - najczęstsze błędy użytkowników
 - ocena przykładowych haseł





Cyberbezpieczny Samorząd

- tworzenie bezpiecznego hasła wg schematu
- c. Reakcja na incydenty: Znajomość procedury zgłoszenie incydentu, dla pracowników.
 - czym jest incydent bezpieczeństwa
 - jak go rozpoznać
 - symulacja incydentu (np. podejrzany e-mail / ransomware)
 - co robić krok po kroku
 - kogo powiadomić
- d. Praca zdalna i urządzenia mobilne: Bezpieczne korzystanie z publicznych sieci Wi-Fi oraz ochrona fizyczna sprzętu służbowego.
- e. Test weryfikujący świadomość zagrożeń i reakcji personelu połączone z prowokacją.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA