Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

CYBERBEZPIECZEŃSTWO DLA PRACOWNIKÓW ADMINISTRACJI PUBLICZNEJ – szkolenie zlecone

- Polecamy organizację **szkolenia zamkniętego** dla Państwa instytucji z zakresu **Cyberbezpieczeństwa dla pracowników administracji publicznej.**
- **Moduły szkoleń są zgodne z wytycznymi projektu „Cyberbezpieczny samorząd".**
- Program, termin, miejsce i forma spotkania podlegają indywidualnym ustaleniom.
- Do wyboru: forma stacjonarna lub online.

Aby otrzymać ofertę szkolenia wystarczy skontaktować się z:

FRDL Małopolski Instytut Samorządu Terytorialnego i Administracji
ul. Floriańska 31, 31-019 Kraków
tel.: 12 623 72 44, 575 850 930
e-mail: szkolenia@mistia.org.pl
Kierownik Zespołu ds. szkoleń:
Magdalena Stawiarska: magdalena.stawiarska@mistia.org.pl

Więcej informacji: www.mistia.org.pl

INFORMACJE O SZKOLENIU:

Cyberbezpieczeństwo w instytucjach publicznych jest niezwykle ważne, ponieważ chroni poufne informacje oraz zapewnia integralność i dostępność usług publicznych. Urząd ze względu na wagę posiadanych informacji stanowi atrakcyjny cel dla różnych rodzajów cyberzagrożeń (wyciek danych, phishing, atak na infrastrukturę). Aby chronić się przed tymi zagrożeniami, urząd powinien stosować środki ochronne takie jak: zabezpieczenia techniczne (np. firewalle i antywirusy), monitoring aktywności w sieci oraz regularne szkolenia pracowników.

Program szkolenia jest zgodny z z wytycznymi projektu „Cyberbezpieczny samorząd".

Szkolenie przeznaczone dla: pracowników działów IT i informatyków odpowiedzialnych za bezpieczeństwo systemów informatycznych, specjalistów ds. bezpieczeństwa informacji i cyberbezpieczeństwa, kierownictwa i kadry zarządzającej, odpowiedzialnych za podejmowanie decyzji dotyczących bezpieczeństwa cybernetycznego, pracowników urzędów i jednostek podległych.

CYBERBEZPIECZEŃSTWO DLA PRACOWNIKÓW ADMINISTRACJI PUBLICZNEJ – Program dla pracowników szeregowych (zgodny z projektem „Cyberbezpieczny samorząd")

1. Bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI.
2. Wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa.
3. Wymagania dla pracowników wynikające z KRI, uoKSC oraz RODO.
4. System Zarządzania Bezpieczeństwem Informacji (SZBI) w praktyce.
5. Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z Internetu.
6. Ochrona informacji i prywatność w Internecie.
7. Ransomware jako poważne zagrożenie dla JST.
8. Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise).
9. Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne.
10. Bezpieczne hasła i uwierzytelnienie dwuskładnikowe.
11. Wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa.

CYBERBEZPIECZEŃSTWO DLA PRACOWNIKÓW ADMINISTRACJI PUBLICZNEJ – Program dla kadry kierowniczej (zgodny z projektem „Cyberbezpieczny samorząd")

1. Podstawy prawne cyberbezpieczeństwa.
2. Wymogi wynikające z KRI, uoKSC i RODO.
3. Przegląd znanych typów ataków na JST.
4. Przegląd nowoczesnych narzędzi i usług cyberbezpieczeństwa (jako wsparcie procesu zakupowego).
5. Zarządzanie ryzykiem w bezpieczeństwie informacji i obszarach technicznych.
6. System Zarzadzania Bezpieczeństwem Informacji – jak skutecznie wdrożyć SZBI.

7. Ciągłość działania – dlaczego jest istotna i jak ją wdrożyć.
8. Współpraca w ramach s46 („System 46”).
9. Identyfikowanie zagrożeń – jak wdrożyć odpowiednie zabezpieczenia.
10. Wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa.
11. Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z Internetu.
12. Ransomware jako poważne zagrożenie dla JST.
13. Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise).
14. Bezpieczne hasła i uwierzytelnienie dwuskładnikowe.

PROWADZĄCY:

audytor, trener, doradca. Specjalista w dziedzinie bezpieczeństwa informacji i cyberzagrożeń. Audytor wiodący normy ISO/IEC 27001:2017. Członek Polskiego Towarzystwa Informatycznego. Prowadzi audyty bezpieczeństwa oraz szkolenia i konsultacje m.in. z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa oraz budowania kultury ochrony informacji.