Program szkolenia online:

Godzina	Zajęcia
8:15	Rejestracja
8:30-10:00	• Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych - zakres regulacji. • Obowiązki podmiotów publicznych w świetle KRI w zakresie procedur i dokumentacji. o System Zarządzania Bezpieczeństwem Informacji w organizacji. o Wyznaczenie osoby do kontaktu. o Incydenty. o Jak właściwie reagować na incydenty. o Podział ról w zakresie bezpieczeństwa informacji w organizacji. o Rozliczalność postępowania a zakres odpowiedzialności. o Działania operacyjne i podejście procesowe. • Procedura audytowa: kto, co, jak i kiedy? • Analiza wymagań i postępowania - jak odczytywać wyniki? • Doskonalenie polityki bezpieczeństwa informacji i cyberbezpieczeństwa. • KRI a ustawa o krajowym systemie cyberbezpieczeństwa. • Bezpieczeństwo systemów teleinformatycznych a ochrona danych osobowych w kontekście RODO.
10:00-10:15	Przerwa
10:15-11:45	• Bezpieczeństwo systemów informatycznych. o Cyberzagrożenia i ataki – zagrożenie XXI wieku. o Cyberprzestępstwa – skala zjawiska. o Możliwe konsekwencje prawne, finansowe i organizacyjne ataku dla funkcjonowania jednostki. • Zagrożenia w sieci. o Typologia ataków oraz ich rodzaje. o Ataki wymierzone w infrastrukturę sieciową. o Ransomware. o Phishing. o Ataki wykorzystujące luki stron internetowych, portali społecznościowych oraz stron. o DDoS. o Ataki ukierunkowane na konkretną osobę / organizację. • Rodzaje szkodliwego oprogramowania. • Czy możemy w pełni zabezpieczyć się przed atakiem? • Człowiek – najsłabsze ogniwo systemu bezpieczeństwa. o Skąd przestępcy czerpią informację na temat obiektu ataku. o Socjotechnika. o Polityka bezpieczeństwa systemów informatycznych. o Które elementy systemów należy chronić najbardziej.
11:45-12:15	Przerwa
12:15-13:45	• Zasady bezpiecznego korzystania z sieci firmowej. o Właściwe zabezpieczenie sieci firnowej. o WiFi – udostępniać czy nie? o Praca zdalna – szanse i zagrożenia. o Jak bezpiecznie korzystać z przeglądarek, bankowości elektronicznej oraz mediów społecznościowych. o Przesyłanie danych ze szczególnym uwzględniałem dokumentów zawierających dane osobowe i dane poufne. o Chmura – czy jest bezpieczna? o Zasady zabezpieczenia stanowiska komputerowego przed niepowołanym dostępem. o Szyfrowanie danych, backup, odzyskiwanie danych. o Uwierzytelniania dwuskładnikowe. o Czy korzystnie z pamięci przenośnych jest bezpieczne?

13:45-14:00	Przerwa

14:00-15:30	• Regulamin użytkownika systemu.
	  ○ Zasady uwierzytelniania.
	  ○ Zasady korzystania z zabezpieczeń.
	  ○ Reagowanie na incydenty w praktyce.
	  ○ Monitorowanie pracy użytkownika.
	• Merytoryczne podsumowanie szkolenia. Sesja pytań i odpowiedzi.