Program szkolenia dla części nr 14: organizacja i przeprowadzenie szkoleń Cyberbezpieczeństwo.

PROGRAM SZKOLENIA:

Dzień zajęć	Temat zajęć	Liczba godzin szkoleniowych	Godziny zajęć	Szczegółowy opis treści zajęć
Dzień 1	Moduł 1: Podstawy cyberbezpieczeństwa i przegląd przepisów	2	**8:00 – 9:30**	• Co to jest cyberbezpieczeństwo? Definicja, znaczenie i wyzwania w kontekście administracji publicznej. • Przegląd przepisów i dyrektyw: RODO, Dyrektywa NIS2, krajowe akty prawne dotyczące cyberbezpieczeństwa. • Pojęcie incydentu bezpieczeństwa: Klasyfikacja, konsekwencje, obowiązek zgłoszenia. • Rola człowieka w cyberbezpieczeństwie: Błędy ludzkie jako główna przyczyna incydentów.
		Przerwa kawowa	**9:30 – 9:40**	
		2	**9:40 – 11:10**	
		Przerwa kawowa	**11:10-11:20**	
	Moduł 2: System zarządzania bezpieczeństwem informacji (ISMS)	2	**11:20 – 12:50**	• Czym jest ISMS? Standardy ISO 27001, cele i korzyści wdrożenia. • Cykl życia ISMS: Planowanie, wdrożenie, utrzymanie, ciągłe doskonalenie. • Elementy ISMS: Polityka bezpieczeństwa, zarządzanie ryzykiem, zarządzanie incydentami, świadomość pracowników. • Praktyczne aspekty wdrożenia ISMS w urzędzie.
		Przerwa obiadowa	**12:50 – 13:20**	
		2	**13:20-14:50**	
Dzień 2		1	**8:00-8:45**	
		1	**8:45-9:30**	• Cel i zakres audytu: Ocena zgodności z przepisami,

	Moduł 3: Audyt bezpieczeństwa systemów informatycznych	*Przerwa kawowa*	**9:30-9:40**	standardami i wewnętrznymi politykami. • Rodzaje audytów: Wewnętrzne, zewnętrzne, specjalistyczne. • Metodyka przeprowadzania audytu: Analiza dokumentacji, testy penetracyjne, wywiady. • Raport z audytu: Zawartość, wnioski, plan działań naprawczych.
		2	**9:40-11:10**	
		Przerwa kawowa	**11:10-11:20**	
	Moduł 4: Bezpieczeństwo sieci i systemów teleinformatycznych	2	**11:20-12:50**	• Zagrożenia dla sieci i systemów: Ataki hakerskie, malware, phishing, ransomware. • Mechanizmy ochrony: Firewall, systemy wykrywania włamań (IDS), systemy zapobiegania włamaniom (IPS). • Bezpieczna konfiguracja systemów: Zasady tworzenia silnych haseł, zarządzanie uprawnieniami. • Bezpieczeństwo urządzeń sieciowych: Routery, switche, punkty dostępowe.
		Przerwa obiadowa	**12:50-13:20**	
		2	**13:20-14:50**	
Dzień 3	Moduł 5: Bezpieczeństwo pracy zdalnej	2	**8:00-9:30**	• Zagrożenia związane z pracą zdalną: Ataki na sieci domowe, utrata urządzeń. • Bezpieczne środowisko pracy zdalnej: VPN, szyfrowanie danych, aktualizacje oprogramowania. • Zarządzanie urządzeniami mobilnymi: Polityka BYOD, zabezpieczenie danych na urządzeniach prywatnych. • Bezpieczna komunikacja zdalna: Konferencje wideo, e-mail.
		Przerwa kawowa	**9:30-9:40**	
		1	**9:40-10:25**	
		1	**10:25-11:10**	• Rola świadomości w ochronie danych: Jakie błędy popełniają użytkownicy? • Szkolenia pracowników: Tematyka, częstotliwość.
		Przerwa kawowa	**11:10-11:20**	
		2	**11:20-12:50**	

	Moduł 6: Świadomość cyberbezpieczeństwa pracowników	*Przerwa obiadowa*	**12:50-13:20**	• Kampanie informacyjne: Budowanie kultury bezpieczeństwa. • Symulacje ataków: Testy weryfikujące skuteczność szkoleń.
		2	**13:20-14:50**	
	Ankieta podsumowująca całość szkolenia	**14:50 – 15:05**		

Projekt „Szkolenie kadr jednostek samorządowych na terenie Subregionu Centralnego Województwa Śląskiego - etap 1” współfinansowanego w ramach programu Fundusze Europejskie dla Śląskiego 2021-2027 (Działanie 5.14 - Usługi rozwojowe dla kadr administracji samorządowej) EFS +.