Harmonogram

Nazwa Beneficjenta: Warmińsko-Mazurski Zakład Doskonalenia Zawodowego w Olsztynie

Placówka realizująca kurs: Centrum Edukacji w Szczytnie

Numer projektu: FEWM.07.06-IZ.00-0001/24

Tytuł projektu: Elastycznie, efektywnie

Nazwa szkolenia zawodowego/kursu: Bezpieczeństwo IT w pracy zdalnej

Nr kursu: 10/130/2025

Uczestników: 1 w tym kobiet: 1, mężczyzn: 0

Termin realizacji: 01.07.2025-01.07.2025

1. Harmonogram

Data realizacji	Godziny realizacji zajęć od-do	Temat zajęć	Wykładowca	Miejsce realizacji zajęć/nazwa instytucji (miejscowość, ulica, nr lokalu, nr sali)
01.07.2025	07:00-07:45	Praca zdalna a powierzchnia ataku – czym różni się od pracy stacjonarnej? Przegląd najczęstszych zagrożeń: phishing, malware, ransomware, sniffing, man-in-the-middle. Wzrost liczby incydentów w czasie pracy zdalnej – dane CERT/CSIRT. Case study: wycieki danych i ataki na firmy w modelu home-office.	Jagłowski Mirosław	ul. Chrobrego 4; Szczytno
	07:45-08:30	Bezpieczne połączenia: VPN, szyfrowanie komunikacji, MFA. Zabezpieczenia urządzeń końcowych (komputer, telefon, drukarka). Szyfrowanie dysków, ochrona hasłem, blokady ekranów. Wymagania dla sieci domowej pracownika. Zasady korzystania z własnych urządzeń (BYOD). Aktualizacje systemów i aplikacji – rola patch managementu.	Jagłowski Mirosław	ul. Chrobrego 4; Szczytno
	08:30-08:35	PRZERWA		
	08:35-09:20	Przegląd narzędzi do bezpiecznej komunikacji i współpracy (Teams, Zoom, Slack – ich ustawienia bezpieczeństwa). Systemy do zarządzania dokumentami (DMS) w środowisku zdalnym. Platformy zdalnego dostępu i wirtualizacji (VDI, RDP, Citrix). Praca w chmurze: Microsoft 365, Google Workspace – ryzyka i zabezpieczenia. Ograniczenia w używaniu nieautoryzowanych aplikacji (shadow IT).	Jagłowski Mirosław	ul. Chrobrego 4; Szczytno

01.07.2025	09:20-10:05	Znaczenie kontroli tożsamości użytkowników w środowisku rozproszonym. Bezpieczne logowanie – silne hasła, polityka rotacji, menedżery haseł. Uwierzytelnianie wieloskładnikowe (MFA) – typy i wdrożenia. Uprawnienia użytkowników – zasada najmniejszych przywilejów. Zarządzanie dostępem do systemów, aplikacji i danych w chmurze. Narzędzia do zarządzania tożsamością: Azure AD, Okta, Keycloak itp.	Jagłowski Mirosław	ul. Chrobrego 4; Szczytno
	10:05-10:10	PRZERWA		
	10:10-10:55	Jak rozpoznać incydent? – nietypowe logowania, utrata danych, szyfrowanie. Procedura zgłaszania incydentu (RODO, CSIRT, wewnętrzne procedury). Dokumentowanie incydentów i komunikacja kryzysowa. Rola pracownika w pierwszej reakcji – czego nie robić? Praktyczne ćwiczenie: analiza przykładowego incydentu. Procedura zgłaszania incydentu.	Jagłowski Mirosław	ul. Chrobrego 4; Szczytno
	10:55-11:40	Codzienne nawyki użytkownika – checklista bezpieczeństwa. Rozpoznawanie prób oszustwa: socjotechnika, fałszywe domeny, spoofing. Edukacja pracowników – jak budować świadomość zagrożeń IT. Praca w przestrzeni publicznej (kawiarnia, pociąg) – jak się chronić. Cyberhigiena: hasła, backupy, prywatność w życiu zawodowym i osobistym.	Jagłowski Mirosław	ul. Chrobrego 4; Szczytno