Możliwość dofinansowania

Szkolenie: Cyberbezpieczeństwo w przedsiębiorstwie

Numer usługi 2025/12/02/34202/3187391

2 400,00 PLN brutto
2 400,00 PLN netto
150,00 PLN brutto/h
150,00 PLN netto/h

PASO DORADZTWO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★ 5,0 / 5

995 ocen

Dobre Miasto / stacjonarna
Usługa szkoleniowa
16 h
23.01.2026 do 24.01.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Pracownicy i kadra zarządzająca firmy
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	22-01-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie uczestników do samodzielnego zapobiegania, wykrywania, zwalczania oraz minimalizowania skutków incydentów naruszających bezpieczeństwo systemów informatycznych istotnych dla funkcjonowania przedsiębiorstwa. Po ukończonym szkoleniu uczestnicy będą potrafili skutecznie obronić się przed współczesnymi atakami w sieci, a także zdobędą umiejętność rozpoznawania najczęściej praktykowanego oszustwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia socjotechniki wykorzystywane przez cyberprzestępców.	Charakteryzuje socjotechniki wykorzystywane przez cyberprzestępców.	Test teoretyczny
Definiuje najważniejszych technik cyberataków.	Charakteryzuje najważniejsze techniki cyberataków.	Test teoretyczny
Charakteryzuje i monitoruje zagrożeniom związanym z cyberprzestępczością.	Omawia zagrożenia związane z cyberprzestępczością.	Test teoretyczny
Planuje i organizuje odpowiednie działania oraz zabezpieczenia w przypadku usiłowania cyberataku.	Planuje odpowiednie działania w przypadku cyberataku.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Usługa jest realizowana w godzinach zegarowych, w trybie 16 godzin. Przerwy są wliczane do procesu kształcenia, a tym samym czasu trwania usługi rozwojowej.

1. Wstęp

* co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa,

* polityka bezpieczeństwa - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola,

* incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować,

normy i standardy bezpieczeństwa - powszechnie stosowane rozwiązania, norma ISO27001.

2. Ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)

* ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców,

* sposoby - pod jakimi pretekstami wyłudza się firmowe dokumenty,

* jak rozpoznać, że jest się celem ataku socjotechnicznego,

* jak prawidłowo reagować na ataki socjotechniczne,

* jak i skąd atakujący zbierają dane na twój temat,

* miejsca, w których zostawiamy swoje dane świadomie i nieświadomie,

* jak świadomie udostępniać informacje w sieci.

3. Atak „na komputery” – objaśnienie

* ataki przez sieci bezprzewodowe (wifi, bluetooth, nfc),

* ataki przez pocztę e-mail (fałszywe e-maile),

* ataki przez strony www - jak nie dać się zainfekować, fałszywe strony,

* ataki przez komunikatory (skype, facebook),

* ataki przez telefon (fałszywe sms-y, przekierowania rozmów, itp.),

* ataki: phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam

4. Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów

* polityka haseł, zarządzanie dostępem i tożsamością - jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych,

* bezpieczeństwo fizyczne - urządzenia, nośniki danych, dokumenty,

* bezpieczna praca z urządzeniami mobilnymi (smartfon, laptop),

* problem aktualnego oprogramowania i kopii zapasowych,

* bezpieczna praca z pakietem biurowym Microsoft Office,

* bezpieczna praca z programem pocztowym,

* bezpieczna praca z przeglądarką internetową,

* zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty).

5. Aspekty prawne

* odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji,

* nieautoryzowane użycie systemów komputerowych,

* rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego,

* dane osobowe i dane wrażliwe.

6. Walidacja

Harmonogram

Liczba przedmiotów/zajęć: 20

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 20 Co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa	Izabela Wrona-Waluś	23-01-2026	08:00	09:00	01:00
2 z 20 Polityka bezpieczeństwa. Incydenty bezpieczeństwa	Izabela Wrona-Waluś	23-01-2026	09:00	10:00	01:00
3 z 20 Ataki „na człowieka” tzw. SOCJOTECHNIKA - ataki socjotechniczne	Izabela Wrona-Waluś	23-01-2026	10:00	11:00	01:00
4 z 20 Przerwa	Izabela Wrona-Waluś	23-01-2026	11:00	11:15	00:15
5 z 20 sposoby pod jakimi pretekstami wyłudza się firmowe dokumenty oraz jak rozpoznać, że jest się celem ataku socjotechnicznego,	Izabela Wrona-Waluś	23-01-2026	11:15	12:00	00:45
6 z 20 jak prawidłowo reagować na ataki socjotechniczne, jak i skąd atakujący zbierają dane na twój temat	Izabela Wrona-Waluś	23-01-2026	12:00	13:00	01:00
7 z 20 miejsca, w których zostawiamy swoje dane świadomie i nieświadomie, jak świadomie udostępniać informacje w sieci	Izabela Wrona-Waluś	23-01-2026	13:00	14:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 20 Atak „na komputery” - ataki przez sieci bezprzewodowe, przez pocztę e-mail, przez strony www	Izabela Wrona-Waluś	23-01-2026	14:00	15:00	01:00
9 z 20 ataki przez komunikatory, ataki przez telefon	Izabela Wrona-Waluś	23-01-2026	15:00	15:30	00:30
10 z 20 ataki: phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam	Izabela Wrona-Waluś	23-01-2026	15:30	16:00	00:30
11 z 20 . Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów-polityka haseł, zarządzanie dostępem i tożsamością	Izabela Wrona-Waluś	24-01-2026	08:00	09:30	01:30
12 z 20 bezpieczeństwo fizyczne, bezpieczna praca z urządzeniami mobilnymi, problem aktualnego oprogramowania i kopii zapasowych	Izabela Wrona-Waluś	24-01-2026	09:30	10:30	01:00
13 z 20 bezpieczna praca z pakietem biurowym Microsoft Office, z programem pocztowym,z przeglądarką internetową	Izabela Wrona-Waluś	24-01-2026	10:30	11:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 20 zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty).	Izabela Wrona-Waluś	24-01-2026	11:30	12:00	00:30
15 z 20 Przerwa	Izabela Wrona-Waluś	24-01-2026	12:00	12:15	00:15
16 z 20 Aspekty prawne- odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji	Izabela Wrona-Waluś	24-01-2026	12:15	13:00	00:45
17 z 20 Aspekty prawne- nieautoryzowane użycie systemów komputerowych	Izabela Wrona-Waluś	24-01-2026	13:00	13:45	00:45
18 z 20 Aspekty prawne- rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego	Izabela Wrona-Waluś	24-01-2026	13:45	14:15	00:30
19 z 20 Aspekty prawne- dane osobowe i dane wrażliwe	Izabela Wrona-Waluś	24-01-2026	14:15	15:00	00:45
20 z 20 Walidacja	-	24-01-2026	15:00	16:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 400,00 PLN
Koszt przypadający na 1 uczestnika netto	2 400,00 PLN

Koszt osobogodziny brutto	150,00 PLN
Koszt osobogodziny netto	150,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Izabela Wrona- Waluś

Trener, doradca, coach; współpracuje z przedsiębiorstwami, instytucjami i podmiotami ekonomii społecznej. Od początku swojej kariery związana ze sprzedażą.
Posiada 15-letnie doświadczenie biznesowe oraz takie samo doświadczenie szkoleniowe.
Ukończyła dwa kierunki studiów oraz studia podyplomowe:
1) Pedagogiczne, Resocjalizacja z elementami profilaktyki na Uniwersytecie Jagiellońskim
2) Pedagogikę Opiekuńczo-Wychowawczą z pracą socjalną na Uniwersytecie Śląskim oraz
3) Akademię Trenerów Biznesu na Uniwersytecie SWPS
Pracowała m.in. jako:
– Dyrektor Regionalny Partner Financial Services (region śląski, małopolski, lubelski, dolnośląski, mazowiecki); zarządzała ok. 200 osobami
– Manager Regionalny w firmie Zepter (region śląski)

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

uczestnik otrzyma materiały szkoleniowe

Adres

ul. Orła Białego 18
11-040 Dobre Miasto
woj. warmińsko-mazurskie

Hotel Kopczyński

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

Paweł Socha

E-mail sochapaw@gmail.com

Telefon (+48) 500 638 265