Możliwość dofinansowania

C4Y KATARZYNA ZASIECZNA

Brak ocen dla tego dostawcy

Szkolenie: CyberTarcza organizacji – ochrona danych i cyberbezpieczeństwo krok po kroku w praktyce

Numer usługi 2026/04/22/203083/3505467

2 300,00 PLN brutto
1 869,92 PLN netto
143,75 PLN brutto/h
116,87 PLN netto/h
196,00 PLN cena rynkowa

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
18.05.2026 do 19.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa szkoleniowa skierowana jest do osób wykonujących pracę zawodową związaną z przetwarzaniem danych osobowych oraz informacji organizacji, w szczególności do: • pracowników i współpracowników organizacji publicznych i prywatnych, • pracowników administracji, kadr, księgowości, sprzedaży, obsługi klienta, sekretariatów i logistyki, • koordynatorów, liderów oraz kierowników zespołów, • osób odpowiedzialnych za obieg dokumentów, komunikację wewnętrzną i zewnętrzną oraz współpracę z kontrahentami, • osób rozpoczynających pracę na stanowiskach wymagających dostępu do danych i informacji organizacji. Szkolenie jest odpowiednie dla uczestników bez specjalistycznej wiedzy technicznej i może być realizowane niezależnie od branży
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	17-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Szkolenie przygotowuje do bezpiecznego przetwarzania danych osobowych oraz informacji organizacji w codziennej pracy poprzez rozwinięcie umiejętności identyfikowania zagrożeń cyberbezpieczeństwa, stosowania zasad bezpiecznej komunikacji i udostępniania informacji, zabezpieczania kont i urządzeń oraz właściwego reagowania na incydenty bezpieczeństwa zgodnie z obowiązującymi procedurami i zasadami cyberhigieny.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje i wyjaśnia zagrożenia cybernetyczne (w tym phishing/BEC) oraz ich skutki dla organizacji.	Wskazuje min. 3 typowe zagrożenia (np. phishing, BEC, ransomware)	Test teoretyczny
	Opisuje min. 2 możliwe skutki (np. przestój, utrata danych, straty finansowe).	Test teoretyczny
Wyjaśnia zasady ochrony danych i informacji organizacji i reguły ograniczania dostępu (need-to-know).	Rozróżnia dane osobowe vs dane firmowe/techniczne	Test teoretyczny
	Wskazuje właściwe zasady postępowania dla min. 3 przykładów informacji/dokumentów	Test teoretyczny
Opisuje ryzyka związane z kontami, stanowiskami współdzielonymi i nośnikami oraz sposoby ich ograniczania.	Wskazuje min. 2 ryzyka oraz min. 2 działania ograniczające ryzyko (np. MFA, zasady haseł, blokada ekranu, zasady dla nośników).	Test teoretyczny
Identyfikuje cechy phishingu/BEC i dobiera właściwe działanie (nie otwiera/ weryfikuje/ zgłasza)	Wskazuje prawidłową reakcję w każdym scenariuszu (np. weryfikacja kanałem niezależnym, zgłoszenie)	Test teoretyczny
Dobiera bezpieczny sposób udostępnienia dokumentu lub informacji (kanał + uprawnienia + zabezpieczenia)	Wskazuje właściwy kanał (mail/chmura/link/druk)	Test teoretyczny
	Dobiera adekwatne zabezpieczenia (uprawnienia, hasło, ograniczenie czasu dostępu)	Test teoretyczny
Wykazuje odpowiedzialność za bezpieczeństwo informacji: stosuje zasady poufności i reaguje na nieprawidłowości	Wskazuje zachowanie zgodne z zasadami poufności i minimalizacji dostępu	Test teoretyczny
	deklaruje i uzasadnia działania ograniczające ryzyko w swoim obszarze pracy	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Współpracuje w zespole w sytuacji incydentu: komunikuje się rzeczowo i przekazuje komplet informacji.	Wskazuje poprawny sposób komunikacji i eskalacji (kogo, kiedy, co przekazać)	Test teoretyczny
	Unika działań ryzykownych (np. „samodzielne naprawy", przekazywanie danych nieuprawnionym)	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie ma charakter teoretyczno-praktyczny (warsztat) i skupia się na sytuacjach, które najczęściej prowadzą do naruszeń bezpieczeństwa: komunikacja e-mail i telefoniczna, udostępnianie dokumentów, praca na kontach i urządzeniach, dostęp do informacji w zespołach, współpraca z kontrahentami oraz reakcja na incydenty. Szkolenie uwzględnia podstawowe obowiązki i zasady wynikające z RODO w codziennej pracy. Uczestnicy pracują na scenariuszach i checklistach, ucząc się rozpoznawać próby wyłudzeń (np. phishing/BEC), dobierać bezpieczne kanały udostępniania danych oraz podejmować właściwe działania w pierwszych minutach incydentu. Efektem jest zestaw praktycznych nawyków i procedur możliwych do wdrożenia od razu po szkoleniu, niezależnie od branży.

Program szkolenia

Moduł 1. Dane i informacja w organizacji – klasyfikacja i poufność

- rodzaje informacji: dane osobowe, informacje organizacji, dokumentacja;
- klasyfikacja informacji i poziomy poufności;
- minimalizacja dostępu (need-to-know), role i odpowiedzialności;
- przechowywanie i obieg dokumentów (wersje, kopie, wydruki);
- ćwiczenie: klasyfikacja informacji i minimalny dostęp dla ról.

Moduł 2. Bezpieczne udostępnianie informacji i dokumentów

- mail/chmura/link/druk – ryzyka i dobre praktyki;
- uprawnienia, kontrola dostępu, czas dostępu, wersjonowanie;
- podstawowe zabezpieczenia (hasła, bezpieczne linki, ograniczenia pobrań);
- ćwiczenie: dobór sposobu udostępnienia w scenariuszach.

Moduł 3. Phishing i oszustwa w korespondencji (BEC) – rozpoznawanie i reakcja

- typowe scenariusze i sygnały ostrzegawcze;
- procedura bezpiecznej weryfikacji (niezależny kanał, potwierdzanie danych);
- eskalacja i zgłaszanie zdarzeń;
- ćwiczenie: analiza przypadków i wybór prawidłowej reakcji.

Moduł 4. Konta, dostępy i cyberhigiena pracy

- hasła, MFA (tam gdzie możliwe), zasady przechowywania;
- konta służbowe i współdzielone, blokada ekranu, wylogowanie;
- nośniki i urządzenia (np. USB) – minimalne zasady bezpieczeństwa;
- ćwiczenie: szybka samoocena stanowiska – checklista nawyków.

Moduł 5. Incydent bezpieczeństwa – pierwsze 15 minut + plan wdrożenia

- co jest incydentem, czego nie robić (typowe błędy);
- procedura pierwszych 15 minut: rozpoznanie → zabezpieczenie → zgłoszenie → ograniczenie skutków;
- minimalny zakres informacji do zgłoszenia;
- checklista wdrożeniowa na 30 dni (3–5 działań do wdrożenia);
- ćwiczenie: praca na scenariuszu incydentu i plan działań.
- Walidacja efektów uczenia - test teoretyczny

Metody dydaktyczne

Wykład na żywo, prezentacja, dyskusja moderowana, praca na scenariuszach, ćwiczenia praktyczne, checklisty i krótkie zadania wdrożeniowe. Zajęcia mają charakter teoretyczno-praktyczny.

Walidacja

Walidacja odbywa się w formie testu (15–25 pytań, w tym pytania scenariuszowe). Kryterium zaliczenia: minimum 70% poprawnych odpowiedzi. Rozdzielność szkolenia od walidacji (rozdzielność osobowa): osoba prowadząca szkolenie nie przeprowadza końcowej walidacji. Wyniki walidacji są dokumentowane protokołem oraz arkuszem oceny/testem.

Czas trwania i organizacja

Łączny czas trwania: 16 godzin dydaktycznych (2 dni po 8 godzin dydaktycznych). Szkolenie realizowane w godzinach dydaktycznych. Przerwy nie są wliczone w czas trwania usługi. Liczba godzin teoretycznych: 7, liczba godzin praktycznych 8 + 1 h walidacja

Materiały dla uczestników

Materiały elektroniczne (prezentacja/skrypt), checklisty, scenariusze ćwiczeń oraz zestaw rekomendacji wdrożeniowych.

Harmonogram

Liczba przedmiotów/zajęć: 10

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Dzień 1: Moduł 1: Otwarcie szkolenia, dane i informacja w organizacji – klasyfikacja i poufność (współdzielenia ekranu, czatu oraz interakcji uczestników)	Anna Kocur-Zychowicz	18-05-2026	09:00	11:15	02:15
2 z 10 Przerwa	Anna Kocur-Zychowicz	18-05-2026	11:15	11:30	00:15
3 z 10 Moduł 2: Bezpieczne udostępnianie informacji i dokumentów (współdzielenia ekranu, czatu oraz interakcji uczestników)	Anna Kocur-Zychowicz	18-05-2026	11:30	13:45	02:15
4 z 10 Przerwa	Anna Kocur-Zychowicz	18-05-2026	13:45	14:30	00:45
5 z 10 Moduł 3 (cz. 1): Phishing i oszustwa w korespondencji (BEC) – rozpoznawanie (współdzielenia ekranu, czatu oraz interakcji uczestników)	Anna Kocur-Zychowicz	18-05-2026	14:30	16:00	01:30
6 z 10 Dzień 2: Moduł 3 (cz. 2): Phishing/BEC – procedura weryfikacji i reakcja +powtórzenie z poprzedniego dnia. (współdzielenia ekranu, czatu oraz interakcji uczestników)	Anna Kocur-Zychowicz	19-05-2026	09:00	10:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 10 Moduł 4: Konta, dostępy i cyberhigiena pracy. (współdzielenia ekranu, czatu oraz interakcji uczestników)	Anna Kocur-Zychowicz	19-05-2026	10:30	13:45	03:15
8 z 10 Przerwa	Anna Kocur-Zychowicz	19-05-2026	12:45	13:30	00:45
9 z 10 Moduł 5: Incydent bezpieczeństwa – „pierwsze 15 minut” + plan wdrożenia (współdzielenia ekranu, czatu oraz interakcji uczestników)	Anna Kocur-Zychowicz	19-05-2026	13:30	15:00	01:30
10 z 10 Walidacja - test teoretyczny	-	19-05-2026	15:00	15:45	00:45

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 300,00 PLN
Koszt przypadający na 1 uczestnika netto	1 869,92 PLN
Koszt osobogodziny brutto	143,75 PLN
Koszt osobogodziny netto	116,87 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Anna Kocur-Zychowicz

Ekspertka w zakresie ochrony danych osobowych i bezpieczeństwa informacji, zawodowo związana z tym obszarem od 2015 roku. Od 2017 r. Administrator Bezpieczeństwa Informacji, a od 2018 r. Inspektor Ochrony Danych w podmiotach publicznych, sektorze prywatnym oraz organizacjach pozarządowych. Doradca w zakresie bezpieczeństwa informacji, wspierający organizacje w budowie, wdrażaniu i doskonaleniu systemów zarządzania oraz spełnianiu wymogów prawnych i normatywnych.
Audytor systemów zarządzania bezpieczeństwem informacji:
– audytor wewnętrzny ISO/IEC 27001 od 2017 r.,
– audytor wiodący ISO/IEC 27001:2022 / 2023-08,
– audytor wiodący ISO 22301:2020 (ciągłość działania).

Doświadczenie w zakresie szkoleń
Wieloletni szkoleniowiec z bardzo dużym doświadczeniem dydaktycznym – około 150 szkoleń rocznie dla administracji publicznej, jednostek organizacyjnych oraz sektora prywatnego. Prowadzi szkolenia z zakresu RODO, bezpieczeństwa informacji, systemów zarządzania bezpieczeństwem oraz audytów wewnętrznych.
Wykształcenie
Absolwentka Uniwersytetu im. Adama Mickiewicza w Poznaniu. Ukończyła studia podyplomowe m.in. w Akademii Leona Koźmińskiego w Warszawie (ochrona danych osobowych i informacji niejawnych), na Uniwersytecie Ekonomicznym we Wrocławiu (audyt wewnętrzny), Uniwersytecie Szczecińskim (pedagogika) oraz Politechnice Koszalińskiej (systemy podatkowe i finanse)

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały elektroniczne (prezentacja/skrypt), checklisty, scenariusze ćwiczeń oraz zestaw rekomendacji wdrożeniowych.

Informacje dodatkowe

- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej
- 1 godzina rozliczeniowa = 45 minut
- przerwy nie wliczają się do czasu szkolenia
- Karta niniejszej usługi rozwojowej została przygotowana zgodnie z obowiązującym Regulaminem Bazy Usług Rozwojowych

Zapisując się na usługę wyrażasz zgodę na rejestrowanie/nagrywanie swojego wizerunku na potrzeby monitoringu, kontroli oraz w celu utrwalenia efektów uczenia się.

Usługa może być zwolniona z VAT dla Uczestników, których poziom dofinansowania wynosi co najmniej 70% na podstawie § 3 ust. 1 pkt. 14 Rozporządzenia Ministrów Finansów z 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień.

Warunki techniczne

Platforma: MS Teams

iOS: iOS 11

Windows: Windows 10 kompilacja 14393

Android: Android OS 5.0

Funkcje sieci Web. Najnowsza wersja przeglądarki Safari, Internet Explorer 11, Chrome, Edge lub Firefox

Komputer Mac: MacOS 10.13

Połączenie internetowe: wymagane jest połączenie internetowe przewodowe lub bezprzewodowe (3G, 4G, LTE) o następujących parametrach:

- dla transmisji wideo w jakości HD 720p minimalna przepustowość łącza internetowego wynosi: 1.5Mbps/1.5Mbps (wysyłanie/odbieranie).

- dla transmisji wideo w jakości FullHD 1080p minimalna przepustowość łącza internetowego wynosi: 3Mbps/3Mbps (wysyłanie/odbieranie).

Okres ważności linku: Link będzie ważny w dniach i godzinach wskazanych w harmonogramie usługi.

Link: będzie udostępniony i umieszczony w karcie na 5 dni roboczych przed szkoleniem.

Kontakt

KATARZYNA ZASIECZNA

E-mail katarzynazasieczna@gmail.com
Telefon (+48) 668 163 580