Możliwość dofinansowania

"LUGA" AGNIESZKA GLIŃSKA

★★★★★

Cyberbezpieczeństwo i ochrona zasobów informatycznych – aspekty organizacyjne i techniczne. Szkolenie dla pracowników firm korzystających z komputera i internetu (10x45 min.)

960,00 PLN brutto
960,00 PLN netto
96,00 PLN brutto/h
96,00 PLN netto/h

Numer usługi 2024/05/29/7321/2165640

zdalna w czasie rzeczywistym
Usługa szkoleniowa
10 h
08.09.2025 do 29.12.2025

Informacje podstawowe

Kategoria	Techniczne / Pozostałe techniczne
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników wsparcie dla osób indywidualnych

Grupa docelowa usługi	Usługa szkoleniowa jest skierowana do praconików firmy, którzy w codziennej pracy pracują z komputerem, np:
	
	Pracownicy administracyjni:
	
	• Osoby odpowiedzialne za administrację i zarządzanie systemami informatycznymi w firmie.
	• Pracownicy biurowi regularnie korzystający z komputerów i internetu w codziennej pracy.
	
	Nowo zatrudnieni pracownicy:
	
	• Osoby nowe w firmie, które muszą zapoznać się z zasadami i praktykami bezpieczeństwa obowiązującymi w organizacji.
	
	Pracownicy działów finansowych i HR:
	
	• Osoby przetwarzające wrażliwe dane finansowe i osobowe, które muszą być świadome zagrożeń i odpowiednich środków ochrony.
	
	• **Menadżerowie i kierownicy działów**:
	
	  • Osoby odpowiedzialne za zarządzanie zespołami, które korzystają z technologii informatycznych.
	  • Menadżerowie działów IT, którzy muszą zapewnić, że ich zespoły stosują najlepsze praktyki w zakresie cyberbezpieczeństwa.
	
	Usługa adresowana również dla Uczestników Projektu "Kierunek – Rozwój".

Minimalna liczba uczestników	8

Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	07-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	10
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do samodzielnego wdrażania rozwiązań organizacyjnych i technicznych podnoszących poziom cyberbezpieczeństwa w organizacji. Szkolenie obejmuje omówienie najnowszych zagrożeń informatycznych i socjotechnicznych, uczy wykrywania oraz prawidłowego reagowania na ataki. Przekazuje wiedzę, która zwiększy bezpieczeństwo infrastruktury IT i podniesie poziom zgodności z wymogami prawnymi dotyczącymi ochrony danych przetwarzanych w przedsiębiorstwie

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Efekt uczenia się: Charakteryzuje podstawowe zagrożenia cyberbezpieczeństwa, w tym zagrożenia socjotechniczne, techniczne i fizyczne	▪ Wymienia główne typy zagrożeń cyberbezpieczeństwa, w tym phishing, malware, ataki na sieci Wi-Fi. ▪ Definiuje pojęcia związane z atakami socjotechnicznymi, takimi jak phishing i spear-phishing.	Test teoretyczny
Ocenia bezpieczeństwo haseł i stosuje zasady ich zarządzania.	Identyfikuje cechy bezpiecznego hasła i opisuje zasady tworzenia oraz zarządzania hasłami.	Test teoretyczny
Monitoruje i analizuje zagrożenia płynące z korzystania z poczty e-mail, stron internetowych oraz komunikatorów.	▪ Rozpoznaje charakterystyczne cechy podejrzanych e-maili oraz złośliwych załączników lub linków. ▪ Identyfikuje zagrożenia na stronach WWW i komunikatorach.	Test teoretyczny
Opisuje zasady bezpiecznej pracy z przeglądarką internetową i programem pocztowym.	▪ Charakteryzuje ustawienia bezpieczeństwa przeglądarki i programu pocztowego. ▪ Opisuje funkcje ochronne przeglądarki, takie jak blokowanie skryptów i zarządzanie plikami cookie.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje zasady bezpiecznej pracy z urządzeniami mobilnymi oraz sieciami bezprzewodowymi.	▪ Opisuje środki zabezpieczające urządzenia mobilne, takie jak blokada ekranu, szyfrowanie i zarządzanie aplikacjami. ▪ Ocenia zasady bezpiecznego korzystania z publicznych sieci Wi-Fi.	Test teoretyczny
Organizuje bezpieczne przechowywanie i usuwanie danych na nośnikach stacjonarnych i przenośnych.	Charakteryzuje techniki szyfrowania danych i bezpiecznego usuwania danych z urządzeń.	Test teoretyczny
Projektuje działania zapobiegawcze, minimalizujące ryzyko cyberataków.	Rozróżnia środki zapobiegawcze, takie jak regularne aktualizacje, tworzenie kopii zapasowych i kontrola dostępu.	Test teoretyczny
Monitoruje zgodność z wymogami normy PN-ISO/IEC 27001:2022.	Identyfikuje podstawowe wymagania normy PN-ISO/IEC 27001:2022 oraz opisuje elementy załącznika A.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Certyfikat ukończenia szkolenia zawiera opis efektów uczenia się. Efekty te przedstawiają konkretne umiejętności, wiedzę i kompetencje, które osoba zdobyła podczas nauki.

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

Tak, dokument (certyfikat) potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji. Ocena bazuje na wcześniej określonych kryteriach, które jasno wskazują, czy osiągnięto zamierzone cele edukacyjne.

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

Po odbytym szkoleniu, uczestnik przystępuje do dobycia egzaminu końcowego. Na certyfikacie znajduje się informacja o zaliczeniu egzaminu. Implementowane mechanizmy zapewniają niezależność i obiektywność procesu walidacji, co gwarantuje jego wiarygodność i przejrzystość.

Program

Celem szkolenia jest przygotowanie uczestników do świadomego i odpowiedzialnego korzystania z zasobów informatycznych organizacji oraz wdrażania praktycznych rozwiązań podnoszących poziom cyberbezpieczeństwa. Uczestnicy szkolenia zdobędą wiedzę na temat aktualnych zagrożeń, takich jak ataki socjotechniczne, złośliwe oprogramowanie, czy wyłudzanie informacji, oraz nauczą się identyfikować te zagrożenia i skutecznie na nie reagować. Szkolenie kładzie również nacisk na znaczenie aktualizacji systemów, polityki haseł, bezpiecznej pracy z narzędziami internetowymi i mobilnymi oraz ochrony danych osobowych. Dzięki przekazanej wiedzy uczestnicy będą potrafili wdrażać i przestrzegać organizacyjnych i technicznych zasad ochrony informacji, zapewniając zgodność z przepisami prawa i standardami ochrony danych, takimi jak norma PN-ISO/IEC 27001:2022.

Zakres wiedzy przekazywanej na szkoleniu:

1. **Podstawy cyberbezpieczeństwa i ochrony danych:**
   - Rozumienie kluczowych pojęć związanych z bezpieczeństwem informacji, danych osobowych oraz podstaw prawnych ochrony danych w kontekście RODO i krajowych przepisów.
   - Zasady zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001:2022, w tym elementy załącznika A.
2. **Rodzaje zagrożeń i techniki ataków:**
   - Zrozumienie zagrożeń cybernetycznych, takich jak ataki phishingowe, ransomware, malware, oraz zagrożenia fizyczne dla zasobów IT.
   - Mechanizmy ataków socjotechnicznych, takich jak wyłudzanie informacji i manipulacje psychologiczne.
3. **Bezpieczne korzystanie z poczty elektronicznej i przeglądarki internetowej:**
   - Zasady rozpoznawania i unikania złośliwych wiadomości e-mail, identyfikowanie zagrożeń na stronach internetowych, ochrona przed phishingiem.
4. **Bezpieczeństwo w pracy z aplikacjami i narzędziami biurowymi:**
   - Praktyczne wskazówki dotyczące bezpiecznej pracy z pakietami biurowymi i oprogramowaniem komunikacyjnym.
   - Znaczenie aktualizacji oprogramowania i zarządzania kopią zapasową danych.
5. **Bezpieczeństwo urządzeń mobilnych i sieci bezprzewodowych:**
   - Zasady zabezpieczania urządzeń mobilnych (smartfonów, tabletów) oraz bezpieczne korzystanie z sieci Wi-Fi, zwłaszcza publicznych.
6. **Polityka haseł i zarządzanie dostępem:**
   - Tworzenie i zarządzanie bezpiecznymi hasłami, w tym stosowanie menedżerów haseł oraz metody ochrony przed kradzieżą haseł i tożsamości.
7. **Przechowywanie i usuwanie danych:**
   - Bezpieczne przechowywanie, archiwizacja oraz trwałe usuwanie danych z urządzeń stacjonarnych i przenośnych (np. pendrive'ów).
8. **Bezpieczny zdalny dostęp do zasobów firmowych:**
   - Korzystanie z VPN i innych zabezpieczeń w celu ochrony danych podczas pracy zdalnej.
9. **Środki zapobiegawcze i reagowanie na incydenty:**
   - Praktyczne działania prewencyjne oraz procedury reagowania na incydenty bezpieczeństwa w organizacji.
10. **Zabezpieczenia techniczne i fizyczne:**
    - Ochrona fizyczna pomieszczeń, w których przetwarzane są dane, oraz zabezpieczenia systemów IT (firewalle, szyfrowanie danych, monitoring).
11. Test teoretyczny z pytaniami otwartymi i wielokrotnego wyboru.- **WALIDACJA**

Warunek niezbędnych do spełnienia, aby realizacja usługi pozwoliła na osiągnięcie głównego celu:

zaliczenie egzaminu końcowego w formie praktycznej.

Wskazanie warunków organizacyjnych dla przeprowadzenia szkolenia,*np. wyposażenie stanowiska, użyte pomoce dydaktyczne (w tym modele wykorzystane w trakcie szkolenia ze wskazaniem ich rodzaju), itp…*

Szkolenie odbywa się online z wykorzystaniem przygotowanych prezentacji.

Szkolenie to jest skierowane do wszystkich poziomów pracowników firmy, ponieważ cyberbezpieczeństwo jest odpowiedzialnością każdego, kto korzysta z komputerów i internetu w ramach swoich obowiązków zawodowych. Celem jest zapewnienie, że wszyscy pracownicy są świadomi zagrożeń oraz wiedzą, jak chronić zasoby informatyczne firmy.

Zajęcia są realizowane w godzinach dydaktycznych. Przerwa nie jest wliczana w całkowity czas szkolenia.

Minimalna i maksymalna liczba uczesników to 5 maksymalna to 20. Realizowane w formie wykładów. Zajęcia odbywają się w formie zajeć on-line (rozmowa z czasie rzeczywistym).

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	960,00 PLN
Koszt przypadający na 1 uczestnika netto	960,00 PLN
Koszt osobogodziny brutto	96,00 PLN
Koszt osobogodziny netto	96,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Adam Bulica

W branży IT od czasów 286 i digduga. Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001, Audytor Wiodący Systemu Zarządzania Ciągłością Działania wg normy PN-EN ISO 22301

Zarządzanie zespołem wdrożeniowców i serwisantów w setkach projektów przy projektowaniu, budżetowaniu, ofertowaniu oraz realizacji. Przeprowadzone kilkadziesiąt szkoleń w zakresie wdrażania i stosowania przepisów RODO, w tym na zlecenie Dekra Polska. Zrealizowane kilkadziesiąt audytów zgodności działania z wymaganiami stawianymi przez RODO, w tym identyfikacja procesów przetwarzania danych osobowych oraz przygotowywanie zaleceń w zakresie procedur dotyczących ochrony danych osobowych, które powinny zostać wdrożone, także na zlecenie Dekra Certification. Wykonane kilkanaście dokumentacji RODO.

Wyższa Szkoła Biznesu w Dąbrowie Górniczej - Ochrona danych osobowych w administracji i biznesie - Inspektor ochrony danych; Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Menedżerskie studia podyplomowe - Executive MBA; Społeczna Wyższa Szkoła Przedsiębiorczości i Zarządzania w Łodzi Studia podyplomowe; Akademia CISCO CCNA; Akademia Ekonomiczna im. Karola Adamieckiego w Katowicach studia podyplomowe, Zarządzanie i Marketing; Fakultatywne Studia Pedagogiczne, na Politechnice Częstochowskiej; Politechnika Częstochowska mgr inż., Informatyka w elektroenergetyce, Ukończone kilkanaście kursów za

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

materiały autorskie

Informacje dodatkowe

Przed zapisem na usługę, prosimy o kontakt.

Warunki techniczne

Warunki techniczne niezbędne do udziału w usłudze: Zajęcia w formie zdalnej prowadzone są przy wykorzystaniu platformy Zoom/Microsoft Teams, Platforma Zoom/Microsoft Teams pozwala min. na kontakt face to face oraz monitoring realizowanej usługi. Aplikacja jest dostępna na wszystkie urządzenia (komputery, smartfony i tablety)

Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika:komputer stacjonarny/laptop/MAC z kamerą, mikrofonem, głośnikami (słuchawki lub zestaw słuchawkowy z mikrofonem) system operacyjny: Windows 7 lub nowszy, MacOS lub Linux, procesor Intel i3 lub AMD A10, minimum 2GB RAM,

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnikdostęp do internetu - prędkość połączenia co najmniej 10 Mbit/s, przeglądarka internetowa Google Chrome, Mozilla Firefox lub Safari, do prawidłowego wyświetlania materiałów szkoleniowych wymagane jest posiadanie czytnika plików PDF,

Kontakt

Agnieszka Glińska

E-mail info@luga.pl
Telefon (+48) 692 547 267