Usługa - Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej

4.9/5 z 2305 ocen

Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej

Numer usługi: 2021/09/29/23562/1187033

Dostawca usług: Centrum Zarządzania Jakością INFOX Spółka z ograniczoną odpowiedzialnością Spółka komandytowa

Dostępność: Usługa otwarta

Forma świadczenia: zdalna w czasie rzeczywistym

Status usługi: odwołana

Identyfikator projektu: Sektor Finanse

PLN

2 400,00 zł netto za osobę
2 952,00 zł brutto za osobę
150,00 zł netto za osobogodzinę
184,50 zł brutto za osobogodzinę

Rodzaj
Usługa szkoleniowa

Kategoria / Podkategoria
Prawo i administracja / Ochrona informacji niejawnych

Dofinansowanie
Tak

od 13.12.2021
do 16.12.2021

Informacje o usłudze

Sposób dofinansowania:	wsparcie dla osób indywidualnych wsparcie dla przedsiębiorców i ich pracowników
Grupa docelowa usługi:	Usługa rozwojowa **„Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej”** adresowana jest do menadżerów, pracowników odpowiedzialnych za zarządzanie operacyjne, bezpieczeństwo, zarządzanie kryzysowe, ochronę zasobów, administratorów i operatorów systemów ochrony, pracowników sektora finansowego, administratorów IT, a także każdego kto jest zainteresowany tematyką cyberbezpieczeństwa. Udział w usłudze rozwojowej umożliwi uczestnikom nabycie wiedzy oraz umiejętności praktycznych dotyczących ochrony przed atakami cyberprzestępców w zakresie bezpiecznego zarządzania danymi w przedsiębiorstwie, włączając w to wrażliwe dane osobowe. Uczestnik zapozna się z zasadami identyfikacji rodzajów zabezpieczeń, a także stosowania wytycznych dotyczących sposobu pracy w sieci.
Minimalna liczba uczestników:	6
Maksymalna liczba uczestników:	15
Data zakończenia rekrutacji:	26-11-2021
Liczba godzin usługi:	16
Podstawa uzyskania wpisu do świadczenia usługi:	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Ramowy program usługi

Usługa rozwojowa **„Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej”** adresowana jest do menadżerów, pracowników odpowiedzialnych za zarządzanie operacyjne, bezpieczeństwo, zarządzanie kryzysowe, ochronę zasobów, administratorów i operatorów systemów ochrony, pracowników sektora finansowego, administratorów IT, a także każdego kto jest zainteresowany tematyką cyberbezpieczeństwa. Udział w usłudze rozwojowej umożliwi uczestnikom nabycie wiedzy oraz umiejętności praktycznych dotyczących ochrony przed atakami cyberprzestępców w zakresie bezpiecznego zarządzania danymi w przedsiębiorstwie, włączając w to wrażliwe dane osobowe. Uczestnik zapozna się z zasadami identyfikacji rodzajów zabezpieczeń, a także stosowania wytycznych dotyczących sposobu pracy w sieci.

PROGRAM USŁUGI:

1. Podstawowe zagadnienia bezpieczeństwa informacji.
2. Definicja cyberprzestrzeni i cyberbezpieczeństwa.
3. Czym jest w instytucji finansowej polityka bezpieczeństwa i jaka jest jej rola.
4. Incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować.
5. Bezpieczeństwo informacji w instytucji finansowej.
6. Prawne aspekty związane z bezpieczeństwem informacji, np. wymagania RODO, aktualne akty prawne.
7. Tworzenie kultury ochrony informacji.
8. Zagrożenia bezpieczeństwa informacji.
9. Cyberzagrożenia.
10. Ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców.
11. Sposoby - pod jakimi pretekstami wyłudza się firmowe dokumenty.
12. Wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego.
13. Reakcja - jak prawidłowo reagować na ataki socjotechniczne, jak i skąd atakujący zbierają dane.
14. Przykłady kradzieży i wycieku danych.
15. Zagrożenia przy korzystaniu z Internetu: poczta e-mail, strony www.
16. Zasady udzielania dostępu do zasobów informacyjnych.
17. Bezpieczeństwo fizyczne (urządzenia, nośniki danych, dokumenty, „czyste biurko").
18. Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop).
19. Problem aktualnego oprogramowania i kopii zapasowych.
20. Bezpieczna praca z pakietem biurowym Microsoft Office.
21. Bezpieczna praca z programem pocztowym, z przeglądarką internetową.
22. Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty).
23. Czy Twoje hasło do systemów informatycznych jest bezpieczne?
24. Jak stworzyć silne hasło i łatwo je zapamiętać.
25. Jak bezpiecznie chronić hasła.
26. Podejrzane e-maile, czyli przykłady realnych zagrożeń, np. Ransomware.
27. Skuteczne metody ochrony przed atakami.
28. Polityka Bezpieczeństwa Informacji jako skuteczne narzędzie ochrony informacji.
29. Skuteczne procedury ochrony danych.
30. Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji.
31. Nieautoryzowane użycie systemów komputerowych, rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego.

Czas trwania:

Usługa rozwojowa **„Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej"** trwa **16** godzin zegarowych, gdzie 1 godzina szkolenia trwa 60 minut.

Informacje dodatkowe:

Usługa rozwojowa **„Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej":**
- może zostać przeprowadzona stacjonarnie,
- może zostać przeprowadzona dla zamkniętej grupy uczestników – szkolenie indywidualne, zamknięte,
- może zostać zrealizowana w innym, dogodnym terminie,

W celu ustalenia szczegółów realizacji zapraszamy do kontaktu mailowego.

Harmonogram usługi

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Podstawowe zagadnienia bezpieczeństwa informacji. (wykład, czat)	13-12-2021	08:00	08:30	00:30
Definicja cyberprzestrzeni i cyberbezpieczeństwa. (wykład, czat, współdzielenie ekranu)	13-12-2021	08:30	09:00	00:30
Czym jest w instytucji finansowej polityka bezpieczeństwa i jaka jest jej rola. (wykład, czat, współdzielenie ekranu)	13-12-2021	09:15	09:45	00:30
Incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować. (wykład, czat)	13-12-2021	09:45	10:15	00:30

Bezpieczeństwo informacji w instytucji finansowej. (wykład, czat, współdzielenie ekranu)	13-12-2021	10:15	10:45	00:30
Prawne aspekty związane z bezpieczeństwem informacji, np. wymagania RODO, aktualne akty prawne. (wykład, czat)	13-12-2021	10:45	11:15	00:30
Tworzenie kultury ochrony informacji. (wykład, czat, współdzielenie ekranu)	13-12-2021	11:15	11:45	00:30
Zagrożenia bezpieczeństwa informacji. (wykład, czat, współdzielenie ekranu)	13-12-2021	11:45	12:15	00:30
Cyberzagrożenia. (wykład, czat, współdzielenie ekranu)	14-12-2021	08:00	08:30	00:30
Ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców. (wykład, czat)	14-12-2021	08:30	09:00	00:30
Sposoby - pod jakimi pretekstami wyłudza się firmowe dokumenty. (wykład, czat, współdzielenie ekranu)	14-12-2021	09:15	09:45	00:30
Wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego. (wykład, czat, współdzielenie ekranu)	14-12-2021	09:45	10:15	00:30
Reakcja - jak prawidłowo reagować na ataki socjotechniczne, jak i skąd atakujący zbierają dane. (wykład, czat)	14-12-2021	10:15	10:45	00:30
Przykłady kradzieży i wycieku danych. (wykład, czat, współdzielenie ekranu)	14-12-2021	10:45	11:15	00:30
Zagrożenia przy korzystaniu z Internetu: poczta e-mail, strony www. (wykład, czat, współdzielenie ekranu)	14-12-2021	11:15	11:45	00:30
Zasady udzielania dostępu do zasobów informacyjnych. (wykład, czat, współdzielenie ekranu)	14-12-2021	11:45	12:15	00:30
Bezpieczeństwo fizyczne (urządzenia, nośniki danych, dokumenty, „czyste biurko”). (wykład, czat)	15-12-2021	08:00	08:30	00:30
Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop). (wykład, czat, współdzielenie ekranu)	15-12-2021	08:30	09:00	00:30
Problem aktualnego oprogramowania i kopii zapasowych. (wykład, czat, współdzielenie ekranu)	15-12-2021	09:15	09:45	00:30

Bezpieczna praca z pakietem biurowym Microsoft Office. (wykład, czat, współdzielenie ekranu)	15-12-2021	09:45	10:15	00:30
Bezpieczna praca z programem pocztowym, z przeglądarką internetową. (wykład, czat, współdzielenie ekranu)	15-12-2021	10:15	10:45	00:30
Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty). (wykład, czat, współdzielenie ekranu)	15-12-2021	10:45	11:15	00:30
Czy Twoje hasło do systemów informatycznych jest bezpieczne? (wykład, czat, współdzielenie ekranu)	15-12-2021	11:15	11:45	00:30
Jak stworzyć silne hasło i łatwo je zapamiętać. (wykład, czat, współdzielenie ekranu)	15-12-2021	11:45	12:15	00:30
Jak bezpiecznie chronić hasła. (wykład, czat, współdzielenie ekranu)	16-12-2021	08:00	09:00	01:00
Podejrzane e-maile, czyli przykłady realnych zagrożeń, np. Ransomware. Skuteczne metody ochrony przed atakami. (wykład, czat)	16-12-2021	09:15	09:45	00:30
Polityka Bezpieczeństwa Informacji jako skuteczne narzędzie ochrony informacji. (wykład, czat)	16-12-2021	09:45	10:45	01:00
Skuteczne procedury ochrony danych. Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji. (wykład, czat)	16-12-2021	10:45	11:15	00:30
Nieautoryzowane użycie systemów komputerowych, rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego. (wykład, czat)	16-12-2021	11:15	12:15	01:00

Główny cel usługi

Cel edukacyjny

Usługa rozwojowa „Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej” przygotowuje do samodzielnej obrony przed cyberatakami, rozpoznawania najczęściej praktykowanych oszustw, zapoznania się z podstawowymi problemami zabezpieczeń sieci komputerowych, systemów komputerowych i aplikacji, poznania znaczenia i istotności haseł oraz wypracowania odpowiednich reakcji na podejrzane incydenty.

Efekty uczenia się

1. Omawia podstawowe zagadnienia bezpieczeństwa informacji.
2. Definiuje cyberprzestrzeń i cyberbezpieczeństwo.
3. Omawia czym jest w instytucji finansowej polityka bezpieczeństwa i jaka jest jej rola.
4. Charakteryzuje incydenty bezpieczeństwa.
5. Omawia bezpieczeństwo informacji w instytucji finansowej.
6. Analizuje prawne aspekty związane z bezpieczeństwem informacji, np. wymagania RODO, aktualne akty prawne.
7. Tworzy kulturę ochrony informacji.

8. Omawia zagrożenia bezpieczeństwa informacji.
9. Definiuje cyberzagrożenia.
10. Analizuje ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji).
11. Omawia ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców.
12. Omawia sposoby pod jakimi pretekstami wyłudza się firmowe dokumenty.
13. Wykrywa jak rozpoznać, że jest się celem ataku socjotechnicznego.
14. Reaguje prawidłowo na ataki socjotechniczne,
15. Omawia przykłady kradzieży i wycieku danych.
16. Ocenia zagrożenia przy korzystaniu z Internetu: poczta e-mail, strony www.
17. Omawia zasady udzielania dostępu do zasobów informacyjnych.
18. Definiuje bezpieczeństwo fizyczne (urządzenia, nośniki danych, dokumenty, „czyste biurko”).
19. Analizuje bezpieczną prace z urządzeniami mobilnymi (smartfon, tablet, laptop).
20. Charakteryzuje problem aktualnego oprogramowania i kopii zapasowych.
21. Omawia bezpieczną pracę z pakietem biurowym Microsoft Office.
22. Monitoruje bezpieczną pracę z programem pocztowym, z przeglądarką internetową.
23. Stosuje techniki kryptograficzne (szyfrowanie, certyfikaty).
24. Analizuje, co sprawia, że hasło jest bezpieczne.
25. Tworzy silne hasło.
26. Bezpiecznie chroni hasła.
27. Analizuje podejrzane e-maile, czyli przykłady realnych zagrożeń, np. Ransomware.
28. Definiuje etyczny hacking.
29. Omawia skuteczne metody ochrony przed atakami.
30. Omawia Politykę Bezpieczeństwa Informacji jako skuteczne narzędzie ochrony informacji.
31. Przedstawia skuteczne procedury ochrony danych.
32. Omawia odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji.
33. Ocenia nieautoryzowane użycie systemów komputerowych oraz rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego.
34. Stosuje zasady komunikacji interpersonalnej.

Sposób weryfikacji osiągnięcia efektów uczenia się

Efekty uczenia się, osiągnięte dzięki udziałowi uczestników w usłudze rozwojowej **„Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej”** zostaną zweryfikowane poprzez przeprowadzenie przez Trenera testu wiedzy wśród uczestników. Test wiedzy zostanie przeprowadzony w pierwszym dniu usługi rozwojowej (PRE TEST) w celu sprawdzenia poziomu wiedzy uczestników przed udziałem w usłudze rozwojowej. W dniu zakończenia usługi rozwojowej, jako jej podsumowanie zostanie przeprowadzony test wiedzy (POST TEST) mający na celu sprawdzenie wiedzy uczestników po zakończeniu udziału w usłudze rozwojowej.

Dodatkowo, osiągniecie efektów uczenia się dzięki udziałowi uczestników w usłudze rozwojowej **„Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej”** zostanie zweryfikowane poprzez ankietę ewaluacyjną po zakończeniu usługi rozwojowej, mającą na celu indywidualne potwierdzenie przez każdego uczestnika usługi rozwojowej stopnia osiągnięcia przez niego danego efektu uczenia się.

Czy usługa prowadzi do nabycia kompetencji?	Tak

Kwalifikacje

Brak wyników.

Cena

Koszt przypadający na 1 uczestnika netto	2 400,00 zł
Koszt przypadający na 1 uczestnika brutto	2 952,00 zł
Koszt osobogodziny netto	150,00 zł
Koszt osobogodziny brutto	184,50 zł

Zajęcia poprowadzą

Brak wyników.

Kontakt

Karolina Gnutek
email: sekretariat@czj-infox.pl
tel: (+48) 518 925 841

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników otrzymuje komplet materiałów w wersji papierowej i/lub elektronicznej.
Każdy z uczestników otrzymuje na swój indywidualny adres mailowy komplet materiałów w wersji elektronicznej – ściśle dopasowany zawartością do harmonogramu szkolenia.
Materiały przygotowane są w formacie: „pdf", „.doc", „.xlsx", ".xls", „.pptx", „.jpg", „.png"
Uczestnicy otrzymają certyfikat i zaświadczenie, potwierdzające, że ukończyli usługę rozwojową.

Informacje dodatkowe

Usługa rozwojowa, która dla uczestnika ma charakter usługi kształcenia zawodowego / przekwalifikowania zawodowego i jest finansowana ze środków publicznych w co najmniej 70% jest zwolniona z podatku VAT na podstawie §3 ust.1 pkt 14 rozporządzenia Ministra Finansów z dn. 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U.2018.701)).
Cena usługi rozwojowej dla 1 uczestnika, który uzyskał dofinansowanie w co najmniej 70% wynosi **2 400,00** zł netto/brutto.
Cena usługi rozwojowej dla uczestników, którzy uzyskali dofinansowanie ze środków publicznych poniżej 70% oraz dla uczestników, którzy nie uzyskali takiego dofinansowania lub usługa rozwojowa nie ma charakteru usługi kształcenia zawodowego / przekwalifikowania zawodowego jest powiększona o podatek VAT (23%).
Cena usługi rozwojowej dla pozostałych (wyżej opisanych) uczestników to **2 400,00** zł netto **+ 552,00** zł 23%VAT = **2 952,00** zł/osoba brutto

Warunki techniczne

Warunki techniczne

Usługa rozwojowa realizowana w formie zdalnej będzie odbywała się w czasie rzeczywistym. Podczas usługi rozwojowej będą wykorzystywane różne elementy: wykład, czat, ćwiczenia, testy, ankiety, udostępnianie ekranu, współdzielenie ekranu, dyskusje i inne.
Warunki techniczne:
a) Rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa rozwojowa:
Usługa rozwojowa "**Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej**" realizowana będzie zdalnie w czasie rzeczywistym przy wykorzystaniu aplikacji „ZOOM".
b) Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:
Komputer (PC lub laptop) lub tablet lub telefon komórkowy:
- Połączenie internetowe - szerokopasmowe przewodowe lub bezprzewodowe (3G lub 4G / LTE)- Głośniki i mikrofon - wbudowany lub wtyk USB lub bezprzewodowy Bluetooth
- Kamera internetowa lub kamera internetowa HD - wbudowana lub wtyczka USB lub kamera HD lub kamera HD z kartą przechwytywania wideo
- Dwurdzeniowy procesor 2 GHz lub szybszy (zalecany 4-rdzeniowy) (i3 / i5 / i7 lub odpowiednik AMD)
- 2GB pamięci RAM (zalecane 4GB)
- System operacyjny Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja) – dla PC lub laptopa
c) Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:
- Stałe łącze internetowe o prędkości 1,5 Mbps (zalecane 2,5 Mbps z obrazem w jakości HD
- 800kbps / 1.0Mbps (góra / dół) dla wysokiej jakości wideo

- W przypadku widoku galerii / lub video HD 720p: 1,5 / 1,5 (góra / dół)
- Odbieranie wideo HD 1080p wymaga 2,5 (w górę / w dół)
- Przesyłanie wideo HD 1080p wymaga 3,0 (w górę / w dół)
- Tylko do udostępniania ekranu (brak miniatury wideo): 50-75
- Do udostępniania ekranu z miniaturą wideo: 50-150
- W przypadku audio VoiP: 60-80
- W przypadku telefonu Zoom: 60-100

d) Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanychtreści i materiałów:

- Przeglądarka internetowa: Google Chrome, Firefox, lub Safari (zaktualizowane do najnowszej wersji)
- Bezpłatna aplikacja „Zoom”
- Programy z możliwością odczytywania dokumentów „pdf”, „.doc”, „.xlsx”, ”.xls”, „.pptx”, „.jpg”, „.png”

e) Okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line.

Link umożliwiający uczestnictwo w usłudze rozwojowej"**Stosowanie zasad cyberbezpieczeństwa w instytucji finansowej**' jest ważny od momentu wysłania na adres mailowy uczestnika zaproszenia na konkretny dzień usługi rozwojowej aż do momentu zakończenia danego dnia usługi rozwojowej. Trener prowadzący usługę rozwojową jest dostępny w dniach i godzinach uwzględnionych w harmonogramie. Do każdego dnia usługi rozwojowej przypisany jest indywidualny link dostępu. Zaproszenie (link) do szkolenia wysyłany jest na indywidualny adres mailowy uczestnika usługi rozwojowej.