Możliwość dofinansowania

Bezpieczeństwo Firm i Instytucji w praktyce - zabezpieczenia dokumentów i plików, ludzi, budynków na wypadek sytuacji kryzysowej. Certyfikowane szkolenie.

1 709,70 PLN brutto
1 390,00 PLN netto
142,48 PLN brutto/h
115,83 PLN netto/h

Centrum Organizacji Szkoleń i Konferencji SEMPER Magdalena Wolniewicz-Kesaria

★★★★½

Numer usługi 2024/07/29/8282/2241653

zdalna w czasie rzeczywistym
Usługa szkoleniowa
12 h
09.12.2024 do 10.12.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób (kadry zarządzającej i pracowników) firm i placówek publicznych zainteresowanych podniesieniem świadomości dotyczącej zabezpieczenia dokumentów i plików, ludzi, budynków na wypadek sytuacji kryzysowej, w tym współczesnych zagrożeń terrorystycznych oraz nabyciem praktycznej wiedzy z zakresu przetrwania w sytuacji kryzysowej (w tym sytuacji terrorystycznej i zakładniczej), czy wydarzeń o charakterze kryminalnym z użyciem broni.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	08-12-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	12
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie kadry zarządzającej oraz pracowników niższego szczebla na wypadek sytuacji kryzysowych zagrażających przede wszystkim życiu i zdrowiu pracowników i osób przebywających w budynkach i na terenie należącym do firmy, instytucji, a także danym w postaci elektronicznej i tradycyjnej, które mogłyby zostać zniszczone lub uszkodzone w wyniku takich sytuacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Kompetencje społeczne: - ocenia jak odpowiednio reagować w różnych sytuacjach związanych z wykonywanym zawodem - identyfikuje własny styl uczenia się i wybiera sposoby dalszego kształcenia, - określa znaczenie komunikacji interpersonalnej oraz potrafi prawidłowo identyfikować i rozstrzygać dylematy związane z wykonywaniem zawodu.	- Umiejętność dostosowania reakcji do różnorodnych kontekstów zawodowych - Wybór adekwatnych metod do dalszego kształcenia.	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się

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

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji

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

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji

Program

- szkolenie trwa 2 dni (łącznie 12h)
- zajęcia odbywają się w godzinach 09.00-15.00 każdego dnia według harmonogramu:

Dzień I

Godz. 09:00 - 09:10 – PRE TEST – do uzupełnienia przed szkoleniem
Godz. 09:10 - 10:30 – szkolenie (rozmowa na żywo, współdzielenie ekranu)

ZAGROŻENIA DLA BEZPIECZEŃSTWA FIRMOWEGO

1. Zagrożenia naturalne (zagrożenia klimatyczne, ekologiczne, biologiczne i inne.).

2. Zagrożenia w cyberprzestrzeni:

a) cyberprzestępczość (hackerstwo, szpiegostwo komputerowe, cyberterroryzm, cyberagresja, phishing, skimming);

b) zagrożenia związane z internetem (włamania, wirusy, ataki konwencjonalne, walka informacyjna);

c) zagrożenia bezprzewodowe;

d) zagrożenia psychospołeczne (przeciążenie technologią i siecią, uzależnienie od komputera, socjomania internetowa);

f) naruszenie prywatności wynikające z działań niekomercyjnych;

g) zagrożenia dla instytucji państwowych.

Godz. 10:30 - 12:00 – szkolenie (rozmowa na żywo, współdzielenie ekranu)

3. Zagrożenia demograficzne (zmiany na rynku pracy, zmiany w targetowaniu i marketingu wynikające ze zmian demograficznych).

4. Zagrożenia makroekonomiczne, zdrowotne, kulturowe, finansowe.

5. Zagrożenia sensu largo (międzynarodowe, narodowe, militarne i pozamilitarne).

6. Zagrożenia informacji i systemów informacyjnych:

a) bierne i czynne;

c) wewnętrzne i zewnętrzne;

d) sprzętowe i programowe;

e) przypadkowe i celowe;

f) ryzyko wirtualnej współpracy.

Godz. 12:00 - 13:30 – szkolenie (rozmowa na żywo, współdzielenie ekranu)

BEZPIECZEŃSTWO FUNKCJONOWANIA ORGANIZACJI. SPOSOBY POSTĘPOWANIA ORAZ PROCEDURY BEZPIECZEŃSTWA.

1.Cyberterroryzm w prawodawstwie międzynarodowym. Uwarunkowania prawne cyberprzestępczości. Instytucje zajmujące się ochroną cyberprzestrzeni.

2.Kultura ochrony informacji w organizacji. Uwarunkowania prawne oraz praktyczne przykłady i rekomendacje w zakresie zapewnienia bezpieczeństwa różnych kategorii informacji prawnie chronionych (dane osobowe, informacje niejawne, tajemnica przedsiębiorstwa). Środki, procedury i metody zabezpieczenia dokumentów:

a) techniczne środki ochrony (urządzenia techniczne, środki programowe, środki kontroli dostępu, środki kryptograficzne);

b) nietechniczne środki ochrony jako forma zabezpieczenia firmy przed zagrożeniami (polityka bezpieczeństwa informacji, zarządzanie ryzykiem, plany awaryjne, plany ochrony, instrukcje zarządzania systemem teleinformatycznym itp.).

Godz. 13:30 - 15:00 – szkolenie (rozmowa na żywo, współdzielenie ekranu, ćwiczenia)

3. Korzyści z wirtualizacji działalności firmy oraz zabezpieczenia działania w cyberprzestrzeni.

4. Odpowiedzialność karna i dyscyplinarna przeciwko ochronie informacji.

Dzień II
Godz. 09:00 - 10:30 – szkolenie (rozmowa na żywo, współdzielenie ekranu)

TERRORYZM, PRZESTĘPCZOŚĆ I PRZESTĘPCZOŚĆ ZORGANIZOWANA. ALGORYTMY POSTĘPOWANIA W SYTUACJI WYSTĄPIENIA ZAGROŻENIA.

1.Terroryzm, przestępczość i przestępczość zorganizowana – źródła, finansowanie, relacja między procesami globalizacyjnymi, a terroryzmem i przestępczością zorganizowaną.

2.Wpływ migracji wewnętrznych i międzykontynentalnych, uchodźstwa, problemów demograficznych, rynku pracy i edukacji, na europejski terroryzm i przestępczość zorganizowaną.

Godz. 10:30 - 12:00 – szkolenie (rozmowa na żywo, współdzielenie ekranu)

3. Największe organizacje terrorystyczne po 2000 roku – ich cele, zamachy i modus operandi.

4. Przeciwdziałanie terroryzmowi na poziomie państwowym i regionalnym.

5. Krajowe programy zapobiegania terroryzmowi. Zakres odpowiedzialności służb państwowych i europejskich.

Godz. 12:00 - 13:30 – szkolenie (rozmowa na żywo, współdzielenie ekranu, ćwiczenia)

6. Praktyczne przykłady przeciwdziałania zagrożeniu ze strony czynnika ludzkiego (przestępstwa związane z danymi, dokumentami, kradzieżą tajemnicy przedsiębiorstwa, terroryzmem, przestępczością zorganizowaną, przestępstwem kryminalnym). Rozpoznawanie zagrożeń:

a) sygnały pozawerbalne wysyłane przez sprawcę;

b) sylwetka statystycznego terrorysty i przestępcy, obiekty i zachowania, które powinny wzbudzić czujność;

c) zasady bezpieczeństwa w miejscach publicznych i w miejscu pracy związane z przestępczością.

7. Procedury i metody w zakresie przeciwdziałaniu zagrożeniu ze strony natury (powódź, pożar, trzęsienie ziemi, duże natężenie wiatru itd.).

Godz. 13:30 - 14:45 – szkolenie (rozmowa na żywo, współdzielenie ekranu, ćwiczenia)

8. Sposoby i algorytmy postępowania w przypadku wystąpienia zagrożenia stanowiącego:

a) podłożenie ładunku wybuchowego;

b) atak bombowy (z wykorzystaniem ładunków wybuchowych);

c) atak z wykorzystaniem broni palnej;

d) ataki biologiczny, chemiczny, radiologiczny. Informowanie służb o ataku terrorystycznym, sytuacji zakładniczej, wydarzeniu kryminalnym lub podłożeniu ładunku wybuchowego.

9. Atak podczas imprezy masowej, w zamkniętej przestrzeni, w miejscu pracy. Sytuacja zakładnicza. Organizacja sprawnej ewakuacji. Organizacja ucieczki. Przygotowanie do użycia siły w samoobronie. Jak zwiększyć szanse przeżycia pozostałych współpracowników i osób w budynku? Pierwsza samopomoc przedmedyczna. Współdziałanie ze służbami ratunkowymi.

Godz. 14:45 - 14:55 – POST TEST – walidacja po szkoleniu
Godz. 14:55 - 15:00 – podsumowanie i zakończenie szkolenia

Szkolenie będzie realizowane w wymiarze 12-godzinnym, gdzie 1 godzina odpowiada godzinie zegarowej (60min.)

Harmonogram

Liczba przedmiotów/zajęć: 2

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 2 Bezpieczeństwo Firm i Instytucji w praktyce	Trener Semper	09-12-2024	09:00	15:00	06:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 2 Bezpieczeństwo Firm i Instytucji w praktyce	Trener Semper	10-12-2024	09:00	15:00	06:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 709,70 PLN
Koszt przypadający na 1 uczestnika netto	1 390,00 PLN
Koszt osobogodziny brutto	142,48 PLN
Koszt osobogodziny netto	115,83 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Trener Semper

Trener Semper

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- otrzymujesz certyfikat wydany przez jedną z wiodących firm szkoleniowych w Polsce
- materiały szkoleniowe w wersji elektronicznej
- masz dostęp do konsultacji poszkoleniowych w formie e-mail do 4 tygodni po zrealizowanym szkoleniu
- otrzymujesz indywidualną kartę rabatową upoważniającą do 10% zniżki na wszystkie kolejne szkolenia stacjonarne i online organizowane przez Centrum Organizacji Szkoleń i Konferencji SEMPER

Warunki uczestnictwa

ZGŁOSZENIE NA USŁUGĘ
Rezerwacji miejsca szkoleniowego można dokonać za pośrednictwem BUR.

Informacje dodatkowe

Metody pracy podczas szkolenia on-line:

- wygodna forma szkolenia - wystarczy dostęp do urządzenia z internetem (komputer, tablet, telefon), słuchawki lub głośniki i ulubiony fotel
- szkolenie realizowane jest w nowoczesnej formie w wirtualnym pokoju konferencyjnym i kameralnej grupie uczestników
- bierzesz udział w pełnowartościowym szkoleniu - Trener prowadzi zajęcia "na żywo" - widzisz go i słyszysz
- pokaz prezentacji, ankiet i ćwiczeń widzisz na ekranie swojego komputera w czasie rzeczywistym.
- podczas szkolenia Trener aktywizuje uczestników zadając pytania, na które można odpowiedzieć w czasie rzeczywistym
- otrzymujesz certyfikat wydany przez jedną z wiodących firm szkoleniowych w Polsce
- masz dostęp do konsultacji poszkoleniowych w formie e-mail do 4 tygodni po zrealizowanym szkoleniu
- otrzymujesz indywidualną kartę rabatową upoważniającą do 10% zniżki na wszystkie kolejne szkolenia stacjonarne i online organizowane przez Centrum Organizacji Szkoleń i Konferencji SEMPER

Warunki techniczne

1. **Platforma /rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa -** Platforma **Zoom** (https://zoom-video.pl/)
2. **Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji -** komputer, laptop lub inne urządzenie z dostępem do internetu
3. **Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik -** minimalna prędkość łącza: 512 KB/sek
4. **Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów** - komputer, laptop lub inne urządzenie z dostępem do internetu. Nie ma potrzeby instalowania specjalnego oprogramowania.
5. **Okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line -** do momentu zakończenia szkolenia
6. Potrzebna jest zainstalowana najbardziej aktualna oficjalna wersja jednej z przeglądarek: **Google Chrome, Mozilla Firefox, Safari, Edge lub Opera**. Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy); 2GB pamięci RAM (zalecane 4GB lub więcej); System operacyjny taki jak Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS. Łącze internetowe o minimalnej przepustowości do zapewnienia transmisji dźwięku 512Kb/s, zalecane min. 2 Mb/s oraz min. 1 Mb/s do zapewnienia transmisji łącznie dźwięku i wizji, zalecane min. 2,5 Mb/s.

Kontakt

Angelika Poznańska

E-mail info@szkolenia-semper.pl
Telefon (+48) 570 590 060