Możliwość dofinansowania

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

Numer usługi 2024/04/08/8282/2116502

1 832,70 PLN brutto
1 490,00 PLN netto
114,54 PLN brutto/h
93,13 PLN netto/h

Centrum Organizacji Szkoleń i Konferencji SEMPER Magdalena Wolniewicz-Kesaria

★★★★½

Kraków / stacjonarna
Usługa szkoleniowa
16 h
08.08.2024 do 09.08.2024

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	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	07-08-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
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?

Otrzymane zaświadczenie po ukończonym szkoleniu zawiera szczegółowe informacje dotyczące osiągniętych efektów edukacyjnych przez uczestnika.

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

Nabyta wiedza poddawana jest ocenie poprzez kończącą zajęcia dyskusję trenera z uczestnikami, bazującą na ściśle określonych kryteriach weryfikacji.

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

Świadectwo potwierdza, że proces walidacji jest niezależny od etapu szkolenia, a obiektywność trenerów przeprowadzających walidację jest zagwarantowana.

Program

Dzień I

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.

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.

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.).

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

4. Odpowiedzialność karna i dyscyplinarna przeciwko ochronie informacji.

Dzień II

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.

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.

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.).

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.

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	08-08-2024	10:00	18:00	08:00
2 z 2 Bezpieczeństwo Firm i Instytucji w praktyce	Trener Semper	09-08-2024	09:00	17:00	08:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 832,70 PLN
Koszt przypadający na 1 uczestnika netto	1 490,00 PLN
Koszt osobogodziny brutto	114,54 PLN
Koszt osobogodziny netto	93,13 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Trener Semper

Trener Semper

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne [autorski podręcznik Uczestnika szkolenia, materiały dodatkowe wykorzystywane podczas warsztatów praktycznych]

Materiały piśmiennicze [notatnik, długopis]

Warunki uczestnictwa

Rezerwacji miejsca szkoleniowego można dokonać za pośrednictwem BUR.

Inwestycja

1490.00zł netto (+23% VAT)

Dla jednostek budżetowych finansujących udział w szkoleniu w minimum 70% lub w całości ze środków publicznych stawka podatku VAT = zw.

Informacje dodatkowe

Materiały dydaktyczne:
Standardowo zestaw materiałów szkoleniowych obejmuje:
-autorski podręcznik Uczestnika szkolenia,
-materiały dodatkowe wykorzystywane podczas warsztatów praktycznych
-materiały piśmiennicze [notatnik, długopis]
-dyplom potwierdzający ukończenie szkolenia
-konsultacje poszkoleniowe
-każdy z Uczestników otrzyma indywidualną kartę rabatową upoważniającą do 10% zniżki na wszystkie kolejne szkolenia otwarte organizowane przez Centrum Organizacji Szkoleń i Konferencji SEMPER

Adres

al. 3 Maja 123/A

30-001 Kraków

woj. małopolskie

W szczególnych przypadkach Organizator zastrzega sobie prawo do zmiany hotelu, w którym odbędzie się szkolenie, na hotel o takim samym lub wyższym standardzie i nie stanowi to zmiany warunków umowy. Wszelkie szczegóły organizacyjne przekazujemy Uczestnikom na 7 dni przed terminem szkolenia.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Udogodnienia dla osób ze szczególnymi potrzebami

Kontakt

Angelika Poznańska

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