Załącznik nr 2 do SWZ

UMOWA NR ..... / 2022

na przeprowadzenie szkolenia w ramach projektu pt. „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury krytycznej" współfinansowanego z Funduszu Bezpieczeństwa Wewnętrznego, realizowanego przez Komendę Wojewódzką Policji z siedzibą w Radomiu

zawarta w dniu …… r. w Radomiu pomiędzy

Skarbem Państwa – Komendą Wojewódzką Policji z siedzibą w Radomiu, adres: ul. 11 Listopada 37/59, 26-600 Radom
REGON: 670897379, NIP: 7962234609,

reprezentowaną przez:
insp. Dariusz Krzesickiego – Zastępcę Komendanta Wojewódzkiego Policji z siedzibą w Radomiu,
przy kontrasygnacie:
mł. insp. Anny Cichockiej – Głównego Księgowego Naczelnika Wydziału Finansów Komendy Wojewódzkiej Policji z siedzibą w Radomiu, zwaną dalej Zamawiającym,

a
……...
……...
……..……
reprezentowaną przez:
……..
……..
……..…
zwanym w dalszej części niniejszej umowy „Wykonawcą"

REGON ..... NIP .....

Umowa zawarta na podstawie przeprowadzonego postępowania o udzielenie zamówieniaw trybie art. 275 pkt 1 zgodnie z ustawą Prawo zamówień publicznych z dnia 11 września 2019 r. (Dz. U. z 2021 r. poz. 1129 z późn. zm.).

Przedmiot umowy

§1

Wykonawca zobowiązuje się przeprowadzić na rzecz Zamawiającego szkolenie CompTIA wraz z wydaniem vouchera na egzamin certyfikacyjny dla 9 osób w ramach projektu pt. „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury

krytycznej" współfinansowanego z Funduszu Bezpieczeństwa Wewnętrznego (nr 80/PL/2020/FBW) zgodnie ze szczegółowym opisem przedmiotu zamówienia – Załącznik Nr 1.

Warunki realizacji umowy

§ 2

1. Wykonawca musi posiadać status autoryzowanego partnera CompTIA.
2. Wykonawca szkolenia zapewni dla każdego uczestnika dostęp do platformy szkoleniowej do komunikacji audio/video dającej możliwość przeprowadzenia na żywo, przy użyciu sieci Internet, zajęć teoretycznych i praktycznych z możliwością udostępniania obrazu z pulpitu zarówno przez prowadzących, jak i uczestników. Indywidualne stanowiska robocze (komputery kursantów) zostaną zapewnione przez Zamawiającego.
3. Wykonawca przeprowadzi szkolenie w języku polskim dla 9 osób w jednym terminie dla każdego z modułów.
4. Wykonawca wyznaczy termin szkolenia dla każdego z modułów.
5. Szkolenie musi obejmować 5 kolejnych dni roboczych od poniedziałku do piątku.
6. Każdy dzień szkoleniowy to 7 godzin zegarowych. Dokładny harmonogram dzienny dla poszczególnych modułów zostanie uzgodniony z Wykonawcą w ramach kontaktów roboczych.
7. Zamawiający wymaga, aby termin kolejnego modułu był wyznaczony nie wcześniej niż po upływie 21 dni kalendarzowych od zakończenia poprzedniego modułu.
8. Wykonawca zapewni akredytowane materiały szkoleniowe CompTIA dla poszczególnych modułów, dla każdego z uczestników szkolenia. Materiały szkoleniowe muszą być przygotowane w języku polskim lub angielskim. Materiały szkoleniowe mogą być w formie papierowej lub w formie elektronicznej. Koszty opracowania, powielenia i transportu materiałów szkoleniowych ponosi Wykonawca. Wykonawca ponosi pełną odpowiedzialność za zgodność merytoryczną oraz aktualność przekazywanych danych/informacji w materiałach szkoleniowych.
9. Wykonawca zapewni konsultacje on-line w zakresie tematyki określonej w szkoleniu do 20 dni po zakończeniu poszczególnego modułu dla każdego z uczestników szkolenia.
10. Każdy uczestnik otrzyma imienny certyfikat ukończenia poszczególnego modułu, sygnowany przez firmę CompTIA.
11. Każdorazowo po zakończeniu poszczególnego modułu Wykonawca zobowiązuje się do przekazania imiennych voucherów dla uczestników szkolenia (modułu) na egzaminy certyfikacyjne CompTIA – odpowiednie dla danego modułu, najpóźniej w dniu zakończenia poszczególnego modułu.

Dokumentacja do umowy i do jej rozliczenia

§ 3

Załącznikami do niniejszej umowy, stanowiącymi jej integralną część są następujące dokumenty:

- szczegółowy opis przedmiotu zamówienia – Załącznik Nr 1,
- wzór ankiety ewaluacyjnej – Załącznik Nr 2,
- wzór oświadczenia wykonawcy dotyczący przekazanych imiennych certyfikatów, materiałów szkoleniowych, imiennych voucherów oraz potwierdzające uczestnictwo w szkoleniu– Załącznik Nr 3,
- wzór protokołu kontroli realizacji umowy – Załącznik Nr 4.

§ 4

Zamawiający wymaga, aby do rozliczenia usługi szkoleniowej Wykonawca przedstawił zgodnie z załączonym wzorem:

1) oświadczenie wykonawcy dotyczące przekazanych imiennych certyfikatów, materiałów szkoleniowych, imiennych voucherów oraz potwierdzające uczestnictwo w szkoleniu;
2) ankiety ewaluacyjne;
3) analizę ankiet ewaluacyjnych.

Termin realizacji umowy

§ 5

1. Wykonawca zobowiązuje się do wykonania szkolenia w przeciągu trzechmiesięcy od daty zawarciaumowy.
2. Szkolenie odbędzie się w trzech terminach, oddzielnie dla każdego modułu.
3. Dokładne terminy szkoleń będą ustalane w kontaktach roboczych z wyłonionym Wykonawcą.

Zobowiązanie stron

§ 6

1. Wykonawca lub Podwykonawca zobowiązuje się do nawiązania stosunku pracy, w rozumieniu art. 22 § 1 ustawy z dnia 26.06.1974 r. – Kodeks pracy, przy wykonywaniu czynności polegających na sporządzaniudokumentacji dot. niniejszego szkolenia (oświadczenia, ankiety ewaluacyjne, zaświadczenia, certyfikaty itp.).
2. Nawiązanie stosunku pracy powinno rozpocząć się nie później niż w dniu rozpoczęcia realizacji umowy i trwać do końca jej realizacji.
3. W przypadku rozwiązania stosunku pracy przez pracownika lub przez pracodawcę przed zakończeniem okresu realizacji umowy, Wykonawca lub Podwykonawca zobowiązuje się do zatrudnieniaw jej miejsce innej osoby, która będzie realizować czynności, o których mowa w ust. 1.
4. W trakcie realizacji przedmiotu umowy Zamawiający uprawniony jest do wykonywania czynności kontrolnych wobec Wykonawcy lub Podwykonawcy odnośnie spełnienia przez Wykonawcę lub Podwykonawcę obowiązku, o którym mowa w ust. 1. Zamawiający w szczególności uprawniony jestdo wezwania Wykonawcy lub Podwykonawcy do przedłożenia Zamawiającemu w wyznaczonym w tym wezwaniu terminie dowodu spełnienia tego obowiązku w postaci:
   1) pisemnego oświadczenia w tym zakresie zawierającego w szczególności: dokładne określenie podmiotu składającego oświadczenie, datę złożenia oświadczenia, wskazanie, że objęte wezwaniem czynności wykonują osoby, z którymi został nawiązany stosunek pracy wraz ze wskazaniem liczby tych osób, rodzaju nawiązanego stosunku pracy i wymiaru etatu oraz podpis osoby uprawnionej do złożenia oświadczenia w imieniu Wykonawcy lub Podwykonawcy;
   2) pisemnego oświadczenia zatrudnionego pracownika potwierdzającego wykonywanie czynności, o których mowa w ust. 1;
   3) potwierdzonych przez Wykonawcę lub Podwykonawcę za zgodność z oryginałem kopii dokumentów stwierdzających nawiązany stosunek pracy osób wykonujących

w trakcie realizacji zamówienia czynności, których dotyczy ww. oświadczenie Wykonawcy lub Podwykonawcy (wraz z dokumentem regulującym zakres obowiązków, jeżeli został sporządzony). Kopie umów o pracę/dokumentu stwierdzającego nawiązany stosunek pracy powinny zastać zanonimizowana w sposób zapewniający ochronę danych osobowych pracowników, zgodnie z przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. z 2019 r. poz. 1781), w szczególności bez adresów, numerów PESEL pracowników. Imię i nazwisko pracownika nie podlega anonimizacji. Informacje takie jak: data nawiązania stosunku pracy, rodzaj nawiązanego stosunku pracy i wymiar etatu powinny być możliwe do zidentyfikowania;

4) dokumentów potwierdzających opłacanie składek na ubezpieczenie społeczne i zdrowotne z tytułu nawiązanego stosunku pracy (wraz z informacją o liczbie odprowadzonych składek), które mogą przyjąć postać zaświadczenia właściwego oddziału ZUS lub zanonimizowanych z wyjątkiem imienia i nazwiska dowodów potwierdzających zgłoszenie pracownika przez pracodawcę do ubezpieczeń.

5. Nie wywiązanie się Wykonawcy lub Podwykonawcy z obowiązku przedłożenia Zamawiającemuw wyznaczonym terminie dowodów, o których mowa w ust. 4, będzie traktowane jako niespełnienie obowiązku zatrudnienia na podstawie umowy o pracę osób, o których mowa w ust. 1 tej umowy.
6. Obowiązek zatrudnienia o którym mowa w ust. 1 zostanie spełniony również poprzez zatrudnienie już wcześniej, przed złożeniem przez Wykonawcęoferty na przedmiotowe zamówienie.
7. Obowiązek zatrudnienia osób, o których mowa w ust. 1 nie dotyczy Wykonawcy lub Podwykonawcy, wyłącznie samodzielnie realizującego czynności wskazane w ust. 1.

Wynagrodzenie i rozliczenie

§ 7

1. Za realizację zamówienia Strony ustalają wynagrodzenie w wysokości ……..… brutto (słownie: ……. złotych).
2. Strony ustalają, że zapłata wynagrodzenia, określonego w ust. 1, nastąpi po realizacji szkolenia składającego się z trzech modułów w terminie 30 dni od daty wpływu do siedziby Zamawiającego prawidłowo wystawionej faktury wraz z dokumentami, o których mowa w § 4.

§ 8

1. Zapłata nastąpi przelewem bankowym na rachunek bankowy Wykonawcy numer: …… ……
2. Za termin zapłaty przyjmuje się obciążenie przez bank rachunku Zamawiającego.
3. Zamawiający posiada konto na Platformie Elektronicznego Fakturowania o numerze PEPPOL GLN 5907714353628.

Ochrona danych

§ 9

1. Wykonawca zobowiązuje się do zachowania w tajemnicy wszelkich informacji i danych osobowych otrzymanych od Zamawiającego w związku z wykonaniem zobowiązań wynikających z Umowy.

2. Strony zobowiązują się do przestrzegania przy wykonaniu Umowy wszelkich postanowień zawartych w obowiązujących przepisach prawnych związanych z ochroną danych osobowych.

3. Wykonawca ponosi odpowiedzialność za zachowanie w tajemnicy wszelkich informacji i danych osobowych przez swoich pracowników lub podwykonawców.
4. Wykonawca odpowiada za ujawnienie, przekazanie, zbycie lub oferowane do zbycia informacji otrzymanych od Zamawiającego, wbrew postanowieniom umowy. Zobowiązanie to wiąże Wykonawcę również po wykonaniu przedmiotu umowy lub jej wypowiedzeniu, bez względu na przyczynę i podlega wygaśnięciu według zasad określonych w przepisach dotyczących zabezpieczania informacji prawnie chronionych.

Zmiany treści umowy

§ 10

Zamawiający zastrzega sobie ze względu na sytuację pandemiczną w kraju lub nieprzewidziane okoliczności uniemożliwiające realizację szkolenia w podanym terminie, możliwość przedłużenia, o maksymalnie sześćmiesięcy, terminu wskazanego w § 5 ust. 1.

Kontrola przebiegu realizacji umowy

§ 11

Zamawiający ma prawo do dokonania kontroli przebiegu i sposobu realizacji umowy poprzez wyznaczenie do udziału w szkoleniu uprawnionego pracownika Zamawiającego, który sporządzi protokół kontroli przebiegu szkolenia – Załącznik Nr 1.

Kary umowne

§ 12

Strony ustalają, iż w razie niewykonania lub nienależytego wykonania umowy przez Wykonawcę, Zamawiający jest uprawniony do naliczenia kary umownej:

1) 1 % wynagrodzenia brutto określonego w § 7 ust. 1 – za każdy stwierdzony przypadek nieprawidłowego wykonywania umowy, wskazany w protokole kontroli przebiegu szkoleniaoraz za nie zachowanie obowiązku zatrudnienia, o którym mowa w § 6 ust. 1;
2) 20 % kwoty wynagrodzenia brutto określonego w § 7 ust. 1 – w przypadku rozwiązania umowy z przyczyn leżących po stronie Wykonawcy.

Łączna wysokość kar umownych nie może przekraczać 20 % wartości brutto, o której mowa w § 7 ust. 1.

Postanowienia końcowe

§ 13

Zamawiający i Wykonawca wybrany w postępowaniu o udzielenie zamówienia obowiązani są współdziałać przy wykonaniu umowy w celu należytej realizacji zamówienia. Do wzajemnego współdziałania przy wykonywaniu niniejszej umowy strony wyznaczają

1) ze strony Zamawiającego: ……....., tel.: ……..., adres e-mail:…….……...……..,
2) ze strony Wykonawcy: ….……...…….……...……

tel.: ……..…….., adres e-mail:…...……...…….…….. .

§ 14

W sprawach nieuregulowanych niniejszą umową mają zastosowanie w szczególności przepisy ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.) oraz ustawy Kodeks cywilny.

§ 15

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 16

Spory między stronami rozstrzyga Sąd właściwy miejscowo dla Zamawiającego.

§ 17

Umowę sporządzono w czterech jednobrzmiących egzemplarzach. Trzy egzemplarze dla Zamawiającego i jeden egzemplarz dla Wykonawcy.

ZAMAWIAJĄCY WYKONAWCA

KONTRASYGNATA

Akceptacja pod względem prawnym

Załącznik Nr 1 do Umowy

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1) Opis przedmiotu zamówienia

Przeprowadzenie szkolenia CompTIA wraz z wydaniem vouchera na egzamin certyfikacyjny dla 9 osób w ramach projektu pt. „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury krytycznej" współfinansowanego z Funduszu Bezpieczeństwa Wewnętrznego (nr 80/PL/2020/FBW).

Szkolenie obejmuje następujące moduły:

1* Przeprowadzenie szkolenia przygotowującego do egzaminu CompTIA Network+ N10 wraz z voucherem na egzamin certyfikacyjny CompTIA Network+ N10 ważnym min. 3 miesiące dni po zakończeniu szkolenia;
2* Przeprowadzenie szkolenia przygotowującego do egzaminu CompTIA Security+ SY0 wraz z voucherem na egzamin certyfikacyjny CompTIA Security+ SY0 ważnym min. 3 miesiące dni po zakończeniu szkolenia;
3* Przeprowadzenie szkolenia przygotowującego do egzaminu CompTIA Cybersecurity Analyst (CySA+) CS0 wraz z voucherem na egzamin certyfikacyjny CompTIA Cybersecurity Analyst (CySA+) CS0 ważnym min. 3 miesiące po zakończeniu szkolenia.

*w wersji kodowej (examcode) najbardziej aktualnej na dzień podpisania umowy

2) Odbiorcy szkolenia

Szkolenie przeznaczone jest dla 9 specjalistów i praktyków z zakresu informatyki śledczej oraz cyberbezpieczeństwa z Wydziałów dw. z Cyberprzestępczością Komend Wojewódzkich Policji. Uczestnikami szkolenia będzie łącznie 9 osób w ramach jednej grupy szkoleniowej.

3) Wymagania ogólne dotyczące realizacji szkolenia

a) Wykonawca musi posiadać status autoryzowanego partnera CompTIA.
b) Wykonawca szkolenia zapewni dla każdego uczestnika dostęp do platformy szkoleniowej do komunikacji audio/video dającej możliwość przeprowadzenia na żywo, przy użyciu sieci Internet, zajęć teoretycznych i praktycznych z możliwością udostępniania obrazu z pulpitu zarówno przez prowadzących, jak i uczestników. Indywidualne stanowiska robocze (komputery kursantów) zostaną zapewnione przez Zamawiającego.
c) Wykonawca przeprowadzi szkolenie w języku polskim
d) Każdy moduł realizowany będzie w ramach jednej grupy szkoleniowej
e) Wykonawca zrealizuje szkolenie w terminie 3 miesięcy od daty podpisania Umowy.
f) Wykonawca wyznaczy termin szkolenia dla każdego z modułów.
g) Szkolenie musi obejmować 5 kolejnych dni roboczych od poniedziałku do piątku.
h) Każdy dzień szkoleniowy to 7 godzin zegarowych. Dokładny harmonogram dzienny dla poszczególnych modułów zostanie uzgodniony z Wykonawcą w ramach kontaktów roboczych.
i) Zamawiający wymaga, aby termin kolejnego modułu był wyznaczony nie wcześniej niż po upływie 21 dni kalendarzowych od zakończenia poprzedniego modułu.
j) Wykonawca zapewni akredytowane materiały szkoleniowe CompTIA dla poszczególnych modułów, dla każdego z uczestników szkolenia. Materiały szkoleniowe muszą być przygotowane w języku polskim lub angielskim. Materiały szkoleniowe mogą być w formie papierowej lub w formie elektronicznej. Koszty opracowania, powielenia i transportu materiałów szkoleniowych ponosi Wykonawca. Wykonawca ponosi pełną odpowiedzialność za zgodność merytoryczną oraz aktualność przekazywanych danych/informacji w materiałach szkoleniowych.
k) Wykonawca zapewni konsultacje on-line w zakresie tematyki określonej w szkoleniu do 20 dni kalendarzowych po zakończeniu każdego z modułów dla każdego z uczestników szkolenia.
l) Uczestnicy otrzymają imienne certyfikaty ukończenia każdego z modułów, sygnowane przez firmę CompTIA.

m) Po zakończeniu każdego z modułów Wykonawca zobowiązuje się do przekazania uczestnikom szkolenia imiennych voucherów na egzaminy certyfikacyjne CompTIA – odpowiednie dla danego modułu, najpóźniej w dniu zakończenia każdego z modułów.

4) Zakres merytoryczny szkolenia (trzy moduły)

Zakres merytoryczny szkolenia musi obejmować wszystkie tematy wyszczególnione w dokumentach „CompTIA Certification Exam Objectives" dla danego typu modułu, dostępnych na oficjalnej stronie CompTIA, to jest:

Moduł 1.:

a) <u>CompTIA Network+</u>

- Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
- Explain the characteristics of network topologies and network types.
- Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
- Given a scenario, configure a subnet and use appropriate IP addressing schemes.
- Explain common ports and protocols, their application, and encrypted alternatives.
- Explain the use and purpose of network services.
- Explain basic corporate and datacenter network architecture.
- Summarize cloud concepts and connectivity options.
- Compare and contrast various devices, their features, and their appropriate placement on the network.
- Compare and contrast routing technologies and bandwidth management concepts.
- Given a scenario, configure and deploy common Ethernet switching features.
- Given a scenario, install and configure the appropriate wireless standards and technologies.
- Given a scenario, use the appropriate statistics and sensors to ensure network availability.
- Explain the purpose of organizational documents and policies.
- Explain high availability and disaster recovery concepts and summarize which is the best solution.
- Explaincommonsecurityconcepts.
- Compare and contrast common types of attacks.
- Given a scenario, apply network hardening techniques.
- Compare and contrast remote access methods and security implications.
- Explain the importance of physical security.
- Explain the network troubleshooting methodology.
- Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.
- Given a scenario, use the appropriate network software tools and commands.
- Given a scenario, troubleshoot common wireless connectivity issues.
- Given a scenario, troubleshoot general networking issues.

Moduł 2.:

b) <u>CompTIA Security+</u>

- Compare and contrast different types of social engineering techniques.
- Given a scenario, analyze potential indicatorsto determine the type of attack.
- Given a scenario, analyze potential indicatorsassociated with application attacks.
- Given a scenario, analyze potential indicatorsassociated with network attacks.
- Explain different threat actors, vectors, and intelligence sources.
- Explain the security concerns associated withvarious types of vulnerabilities.
- Summarize the techniques used in security assessments.
- Explain the techniques used in penetration testing.
- Explain the importance of security conceptsin an enterprise environment.
- Summarize virtualization and cloud computing concepts.
- Summarize secure application development,deployment, and automation concepts.
- Summarize authentication and authorization design concepts.
- Given a scenario, implement cybersecurity resilience.
- Explain the security implications of embedded and specialized systems.

- Explain the importance of physical security controls.
- Summarize the basics of cryptographic concepts.
- Given a scenario, implement secure protocols.
- Given a scenario, implement host or application security solutions.
- Given a scenario, implement secure network designs.
- Given a scenario, install and configure wireless security settings.
- Given a scenario, implement secure mobile solutions.
- Given a scenario, apply cybersecurity solutions to the cloud.
- Given a scenario, implement identity andaccount management controls.
- Given a scenario, implement authenticationand authorization solutions.
- Given a scenario, implement public key infrastructure.
- Given a scenario, use the appropriate tool toassess organizational security.
- Summarize the importance of policies, processes,and procedures for incident response.
- Given an incident, utilize appropriate dataources to support an investigation.
- Given an incident, apply mitigation techniquesor controls to secure an environment.
- Explain the key aspects of digital forensics.
- Compare and contrast various types of controls.
- Explain the importance of applicable regulations, standards, orframeworks that impact organizational security posture.
- Explain the importance of policies to organizational security.
- Summarize risk management processes and concepts.
- Explain privacy and sensitive data concepts in relation to security.

Moduł 3.:

c) <u>CompTIA Cybersecurity Analyst (CySA+)</u>

- Explain the importance of threat data and intelligence.
- Given a scenario, utilize threat intelligenceto support organizational security.
- Given a scenario, perform vulnerability management activities.
- Given a scenario, analyze the output fromcommon vulnerability assessment tools.
- Explain the threats and vulnerabilities associatedwith specialized technology.
- Explain the threats and vulnerabilitiesassociated with operating in the cloud.
- Given a scenario, implement controls to mitigateattacks and software vulnerabilities.
- Given a scenario, apply security solutionsfor infrastructure management.
- Explain software assurance best practices.
- Explain hardware assurance best practices.
- Given a scenario, analyze data as part of security monitoring activities.
- Given a scenario, implement configuration changesto existing controls to improve security.
- Explain the importance of proactive threat hunting.
- Compare and contrast automation concepts and technologies.
- Explain the importance of the incident response process.
- Given a scenario, apply the appropriate incident response procedure.
- Given an incident, analyze potential indicators of compromise.
- Given a scenario, utilize basic digital forensics techniques.
- Understand the importance of data privacy and protection.
- Given a scenario, apply security concepts insupport of organizational risk mitigation.
- Explain the importance of frameworks,policies, procedures, and controls.

Załącznik Nr 2 do Umowy

ANKIETA EWALUACYJNA

DANE O SZKOLENIU

Temat	**Szkolenie obejmujące trzy moduły z zakresu specjalistycznych obszarów informatycznych dla 9 osób w ramach projektu pt. „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury krytycznej" współfinansowanego z Funduszu Bezpieczeństwa Wewnętrznego: 1. moduł szkoleniowy przygotowujący do egzaminu CompTIA Network+ N10* 2. moduł szkoleniowy przygotowujący do egzaminu CompTIA Security+ SY0* 3. moduł szkoleniowy przygotowujący do egzaminu CompTIA Cybersecurity Analyst (CySA+) CS0***
Data	

*w wersji kodowej (examcode) najbardziej aktualnej na dzień podpisania umowy.

SPOSÓB PROWADZENIA SZKOLENIA

1. Czy, Pani/Pana zdaniem, sposób prowadzenia szkolenia z wykorzystaniem formuły nauczania zdalnego – distance learning (dLearning) umożliwił Pani/Panu nabycie wiedzy/umiejętności?

TAK	NIE	CZĘŚCIOWO

2. Jak ocenia Pani/Pan przygotowanie prowadzącego i prezentowany poziom wiedzy?

1	2	3	4	5
bardzo nisko	Nisko	Przeciętnie	wysoko	bardzo wysoko

3. Jak ocenia Pani/Pan umiejętności trenera w przekazywaniu wiedzy i zainteresowania słuchaczy problematyką szkolenia?

1	2	3	4	5
bardzo nisko	Nisko	Przeciętnie	wysoko	bardzo wysoko

4. Jak ocenia Pani/Pan dedykowaną do szkolenia platformę szkoleniową oraz program do wideokonferencji?

1	2	3	4	5
bardzo nisko	Nisko	przeciętnie	wysoko	bardzo wysoko

MATERIAŁY

5. Jak ocenia Pani/Pan przygotowane materiały szkoleniowe?

1	2	3	4	5
bardzo nisko	Nisko	przeciętnie	wysoko	bardzo wysoko

ORGANIZACJA SZKOLENIA

6. Czy Pani/Pana zdaniem czas trwania szkolenia był odpowiedni?

TAK	NIE	CZĘŚCIOWO

OGÓLNA OCENA SZKOLENIA

1	2	3	4	5
bardzo niska	niska	przeciętna	wysoka	bardzo wysoka

ZNACZENIE SZKOLENIA W PRAKTYCE

7. Jaką najbardziej użyteczną wiedzę lub umiejętności nabył/a Pani/Pan podczas szkolenia?

.....
.....
.....
.....

8. W realizacji jakich zadań służbowych wykorzysta Pani/Pan zdobytą wiedzę?

.....
.....
.....
.....

INNE UWAGI I SUGESTIE

.....
.....
.....
.....

Załącznik Nr 3 do Umowy

…… (miejscowość), dnia …… 2022 roku

……
(nazwa i adres Wykonawcy szkolenia / pieczęć firmowa)

OŚWIADCZENIE WYKONAWCY
dotyczący przekazanych imiennych certyfikatów, materiałów szkoleniowych, imiennych voucherów oraz potwierdzające uczestnictwo w szkoleniu

Oświadczam, że firma …….. jako organizator cyklu szkoleń specjalistycznych doskonalących umiejętności z zakresu informatyki śledczej, realizowanych w ramach II modułu projektu „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury krytycznej", przeszkoliła następującą liczbę osób w trybie distance learning:

- 9 osób w ramach tematu „CompTIA Network+ N10*", w terminie …… 2022 roku,
- 9 osób w ramach tematu „CompTIA Security+ SY0*", w terminie …… 2022 roku,
- 9 osób w ramach tematu „CompTIA Cybersecurity Analyst (CySA+) CS0*", w terminie …… 2022 roku,

* w wersji kodowej (examcode) najbardziej aktualnej na dzień podpisania umowy

oraz przekazała wszystkim uczestnikom każdego ze szkoleń imienny certyfikat ukończenia szkolenia, materiały szkoleniowe, imienne vouchery na egzamin certyfikacyjny dla każdego z trzech modułów szkoleniowych.

……
(podpis osoby reprezentującej Wykonawcę,
pieczęć firmowa)

Załącznik nr 4 do Umowy

PROTOKÓŁ KONTROLI REALIZACJI UMOWY

Lp.	Elementy szkolenia podlegające kontroli	TAK	NIE
1.	Przygotowanie dedykowanej do szkolenia platformy szkoleniowej oraz programu do wideokonferencji,zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1 do umowy.		
2.	Udostępnienie i przekazanie uczestnikom szkolenia akredytowanych szkoleniowych materiałów CompTIA przygotowanych w języku polskim lub angielskim dla poszczególnych modułów szkoleniowych, w formie papierowej lub elektronicznej, zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1 do umowy.		
3.	Przeprowadzenie realizacji zajęć teoretycznychw języku polskim dlaposzczególnych modułów szkoleniowych, zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1 do umowy.		
4.	Przeprowadzenie realizacji zajęć praktycznych w języku polskim(ćwiczeń/laboratorium) dla poszczególnych modułów szkoleniowych, zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1 do umowy.		
5.	Przekazanie imiennych certyfikatów ukończenia szkolenia, sygnowanych przez firmę CompTIAdla poszczególnych modułów szkoleniowych, zgodnie z obowiązującymi przepisami dotyczącymi danych osobowych.		
6.	Przekazanie imiennych voucherówna egzamin certyfikacyjny, umożliwiających przeprowadzenie go w języku polskim lub angielskim jednorazowo dla każdego z uczestników poszczególnych modułów szkoleniowych, zgodnie z obowiązującymi przepisami dotyczącymi danych osobowych oraz zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1 do umowy.		
7.	Zapewnienie konsultacji on-line do 20 dni po zakończeniu poszczególnego modułu szkoleniowego dla każdego z uczestników szkolenia, zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1 do umowy.		

UWAGI:

Osoba wyznaczona
ze strony Wykonawcy

Osoba wyznaczona
ze strony Zamawiającego