Projektowane postanowienia umowy (PPU)

§ 1

Przedmiot Umowy

1. W ramach Umowy, Wykonawca zobowiązuje się na rzecz Zamawiającego do:
   1.1. przeprowadzenia szkolenia przygotowującego do egzaminu Certified Information Systems Security Professional (CISSP) dla jednej osoby.
2. Szczegółowy Opis Przedmiotu Zamówienia zawiera Załącznik nr 1 do umowy.
3. Miejsce przeprowadzenia szkoleń pozostaje do wyboru Wykonawcy, z zastrzeżeniem, że musi się znajdować na terenie Warszawy.

§ 2

Termin realizacji Umowy

1. W terminie do 5 dni roboczych od zawarcia Umowy, Wykonawca jest zobowiązany do wskazania co najmniej jednego terminu przeprowadzenia szkolenia do wyboru Zamawiającego.
2. Wykonawca zobowiązuje się do przeprowadzenia szkolenia w terminie nie później niż do 31 października 2021 roku.
3. Przeprowadzenie szkolenia zostanie potwierdzone odpowiednim protokołem, podpisanym przez Zamawiającego, w terminie do 7 dni od dnia zakończenia szkolenia, zgodnie ze wzorem stanowiącym Załącznik nr 2 do Umowy.

§ 3

Wynagrodzenie oraz warunki płatności

1. Za wykonanie całego przedmiotu umowy, Zamawiający zapłaci Wykonawcy wynagrodzenie w wysokości …… zł brutto/ (słownie: ……).
2. Wynagrodzenie całkowite określone w ust. 1 zawiera wszelkie koszty związane z realizacją Umowy, w tym opłaty, podatki i należności wynikające z obowiązujących przepisów prawa, jak również koszt przeprowadzenia szkolenia, zgodnie z wyszczególnionymi w Opisie Przedmiotu Zamówienia wytycznymi.
3. Podstawą do wystawienia faktury będzie podpisany bez zastrzeżeń przez Zamawiającego odpowiedni protokół odbioru.
4. Płatność dokonana będzie na podstawie faktury wystawionej na Ministerstwo Sprawiedliwości, al. Ujazdowskie 11, 00-950 Warszawa, NIP 5261673166, przelewem bankowym z rachunku Zamawiającego na rachunek Wykonawcy wskazany na fakturze, w terminie 21 dni od otrzymania prawidłowo wystawionej faktury.
5. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.

§ 4

Osoby do kontaktu

1. Ze strony Zamawiającego, osobami odpowiedzialnymi za realizację Umowy oraz upoważnionymi do kontaktu i do podpisania protokołów odbioru są:
   - …… tel. ……, e-mail ……,
   - …… tel. ……, e-mail ……. .

2. Ze strony Wykonawcy, osobą odpowiedzialną za realizację Umowy oraz upoważnionymi do kontaktów jest:
   - …… tel. ……, e-mail ……. .
3. Zmiana osób i danych wskazanych w ust. 1 i 2 nie wymaga zawarcia aneksu do Umowy i dla swej skuteczności wymaga pisemnego powiadomienia drugiej Strony.

§ 5

Obowiązki Wykonawcy

1. Wykonawca oświadcza, że posiada wszelkie niezbędne kwalifikacje, uprawnienia, doświadczenie i środki materialne oraz urządzenia niezbędne do wykonania Umowy.
2. Wykonawca zobowiązuje się do wykonania Przedmiotu Umowy zgodnie z parametrami i wymaganiami określonymi w Załączniku nr 1 do Umowy.
3. Wykonawca ponosi całkowitą odpowiedzialność za skutki działania lub zaniechania osób, przy udziale których lub z pomocą których realizuje niniejszą Umowę.
4. Wykonawca zobowiązany jest wykonać Umowę z zachowaniem najwyższej staranności wymaganej od czołowych przedsiębiorców świadczących na terytorium Rzeczypospolitej Polskiej usługi szkoleniowe.
5. Wykonawca ponosi całkowitą odpowiedzialność za własne działania lub zaniechania związane z realizacją Umowy, chyba że szkoda nastąpiła wskutek siły wyższej albo wyłącznie z winy Zamawiającego lub osoby trzeciej.
6. Wykonawca oświadcza, że wszystkie dostarczone materiały szkoleniowe stanowią jego wyłączną własność i nie są obciążone prawami osób trzecich.
7. Przeniesienie przez Wykonawcę jakichkolwiek praw lub zobowiązań związanych z wykonaniem Umowy na osobę trzecią wymaga pisemnej zgody Zamawiającego pod rygorem nieważności.

§ 6

Odpowiedzialność za niewykonanie lub nienależyte wykonanie Umowy

1. Wykonawca zapłaci Zamawiającemu karę umowną:
   1.1. za odstąpienie Wykonawcy od Umowy z przyczyn niezależnych od Zamawiającego albo w przypadku odstąpienia przez Zamawiającego od Umowy z przyczyn leżących po stronie Wykonawcy – w wysokości 20% całkowitego wynagrodzenia brutto określonego w § 3 ust. 1,
   1.2. w razie opóźnienia w wykonaniu przedmiotu umowy w terminie określonym w § 2 ust. 2 - w wysokości 0,5% całkowitego wynagrodzenia brutto określonego w § 3 ust. 1 za każdy dzień opóźnienia,
   1.3. w przypadku ujawnienia jakiejkolwiek informacji lub innego naruszenia bezpieczeństwa informacji w okresie obowiązywania Umowy lub po wygaśnięciu lub rozwiązaniu Umowy – w wysokości 10% całkowitego wynagrodzenia brutto określonego w § 3 ust. 1 za każdy stwierdzony przypadek ujawnienia informacji lub innego naruszenia bezpieczeństwa informacji.
2. Zamawiający ma prawo na zasadach ogólnych dochodzić odszkodowania przenoszącego wysokość zastrzeżonych kary umownej.
3. Kary umowne mogą być naliczane niezależnie i podlegają sumowaniu.
4. Strony ustalają, iż naliczona przez Zamawiającego kara umowna może być przez niego potracona z wynagrodzenia należnego Wykonawcy, wskazanego w § 3 ust. 1, na co niniejszym Wykonawca wyraża nieodwołalną zgodę.

§ 7

Bezpieczeństwo Informacji

1. Informacją w rozumieniu Umowy są wszystkie dane, materiały lub dokumenty, pisemne, elektroniczne lub ustne, przekazane lub pozyskane przez Wykonawcę w związku z realizacją Umowy oraz wytworzone przez Wykonawcę na potrzeby realizacji Umowy.
2. Informacje stanowią wyłączną własność Ministerstwa Sprawiedliwości.
3. Wykonawca może przetwarzać powierzone mu przez Zamawiającego informacje tylko przez okres obowiązywania Umowy.
4. Wykonawca zobowiązuje się po zakończeniu realizacji Umowy do zwrotu Zamawiającemu wszelkich udostępnionych oraz wytworzonych przez siebie w związku z realizacją Umowy informacji, wraz z nośnikami. W przypadku utrwalenia na nośnikach należących do Wykonawcy informacji uzyskanych w związku z realizacją Umowy, Wykonawca zobowiązuje się do usunięcia z nośników tych informacji, w tym również sporządzonych kopii zapasowych, oraz zniszczenia wszelkich danych, dokumentów mogących posłużyć do odtworzenia, w całości lub części, informacji.
5. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji, a także sposobów zabezpieczenia informacji, zarówno w trakcie trwania niniejszej Umowy, jak i po jej wygaśnięciu lub rozwiązaniu. Wykonawca ponosi pełną odpowiedzialność za zachowanie w tajemnicy ww. informacji przez osoby, którymi się posługuje przy realizacji Umowy.
6. Wykonawca zobowiązany jest do zastosowania wszelkich niezbędnych środków technicznych i organizacyjnych zapewniających ochronę przetwarzania informacji, a w szczególności powinien zabezpieczyć informacje przed ich udostępnieniem osobom nieuprawnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem postanowień Umowy, zmianą, utratą, uszkodzeniem lub zniszczeniem.
7. Wykonawca zobowiązuje się do dołożenia najwyższej staranności w celu zabezpieczenia informacji przed bezprawnym dostępem, rozpowszechnianiem lub przekazaniem osobom trzecim.
8. Wykonawca zobowiązany jest zapewnić wykonanie obowiązków w zakresie bezpieczeństwa informacji, w szczególności dotyczącego zachowania w tajemnicy informacji, także przez jego pracowników oraz osoby, które realizują Umowę w imieniu Wykonawcy. Odpowiedzialność za naruszenie powyższego obowiązku spoczywa na Wykonawcy. Naruszenie bezpieczeństwa informacji, w szczególności ujawnienie jakiejkolwiek informacji w okresie obowiązywania Umowy, uprawnia Zamawiającego do odstąpienia od Umowy.
9. Wykonawca może udostępniać informacje jedynie tym swoim pracownikom, którym będą one niezbędne do wykonania powierzonych im czynności i tylko w zakresie, w jakim muszą mieć do nich dostęp dla celów określonych w niniejszej Umowie.
10. Wykonawca ponosi wszelką odpowiedzialność, tak wobec osób trzecich, jak i wobec Zamawiającego, za szkody powstałe w związku z nienależytą realizacją obowiązków dotyczących informacji.
11. Wykonawca zobowiązuje się do ścisłego przestrzegania warunków niniejszej Umowy, które wiążą się z ochroną informacji, w szczególności nie może bez pisemnego upoważnienia Zamawiającego wykorzystywać informacji w celach niezwiązanych z realizacją Umowy.
12. Wykonawca może przetwarzać informacje tylko w wersji elektronicznej.

13. W przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji lub z naruszeniem obowiązków wynikających z Umowy, Zamawiający może przeprowadzić kontrolę wykonywanych przez Wykonawcę czynności. Kontrola może być realizowana przez Zamawiającego lub podmioty przez niego uprawnione.
14. Wykonawca zobowiązany jest współpracować z Zamawiającym w odpowiednim zakresie z podmiotami przeprowadzającymi kontrolę.
15. Wyniki kontroli zostaną przekazane Wykonawcy po jej zakończeniu. Zamawiający może wskazać niezbędne działania, jakie Wykonawca musi podjąć w celu wprowadzenia określonych zmian lub podjęcia określonych czynności.
16. Wykonawca zobowiązany jest do natychmiastowego powiadamiania o nieuprawnionym ujawnieniu lub udostępnieniu informacji oraz o innym naruszeniu bezpieczeństwa informacji, a następnie raportowania Zamawiającemu o podjętych działaniach w powyższym zakresie:
    1) telefonicznie, na numer telefonu ……;
    2) na adres email ……;
    3) faksem, na numer …….. .

    Powiadomienie dokonane telefonicznie musi zostać potwierdzone poprzez jeden ze sposobów wskazanych w pkt 2 – 3 w terminie jednej godziny od dokonania powiadomienia.
17. Wykonawca nie może zwielokrotniać, rozpowszechniać, korzystać w celach niezwiązanych z realizacją Umowy oraz ujawniać informacji osobom trzecim, bez uzyskania w powyższym zakresie pisemnej zgody Zamawiającego, o ile takie informacje nie zostały już podane do publicznej wiadomości lub nie są publicznie dostępne.
18. Wykonawca zobowiązany jest:
    1) zapewnić kontrolę nad tym, jakie informacje, kiedy, przez kogo oraz komu są przekazywane, zwłaszcza gdy przekazuje się je za pomocą teletransmisji danych;
    2) zapewnić, aby osoby, o których mowa w pkt 1, zachowywały w tajemnicy informacje oraz sposoby ich zabezpieczeń.
19. Wykonawca nie może powierzyć przetwarzania informacji innym podmiotom bez uprzedniego uzyskania w tym przedmiocie pisemnej zgody Zamawiającego.
20. W przypadku powierzenia przez Wykonawcę informacji, Wykonawca odpowiada za działania i zaniechania tych podmiotów, jak za własne działania lub zaniechania.
21. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji uzyskanych przez niego w związku z zawarciem Umowy. Wykonawca ponosi pełną odpowiedzialność za zachowanie w tajemnicy ww. informacji przez podmioty, przy pomocy których wykonuje Umowę.
22. Wykonawca zobowiązany jest zapewnić wykonywanie postanowień umownych przez podwykonawców na takich samych warunkach jak określone w niniejszej Umowie.

§ 8

Zmiany umowy

1. Zmiana Umowy może nastąpić w zakresie zasad bezpieczeństwa informacji i odpowiedzialności za naruszenie powyższych zasad w przypadku zmian wymagań bezpieczeństwa informacji obowiązujących u Zamawiającego.
2. Wszelkie zmiany Umowy, jej uzupełnienie lub rozwiązanie za zgodą obu stron, jak również odstąpienie od niej albo za jej wypowiedzenie wymaga zachowania formy pisemnej, pod rygorem nieważności.

§ 9

Odstąpienie od Umowy

1. Zamawiający może odstąpić od części lub całości Umowy w przypadkach określonych w przepisach obowiązującego prawa, w szczególności Kodeksu cywilnego.
2. Jeżeli Wykonawca opóźnia się z rozpoczęciem lub zakończeniem wykonania Umowy tak dalece, że nie jest prawdopodobne, żeby zdołał ją ukończyć w czasie umówionym, Zamawiający może, bez wyznaczenia terminu dodatkowego, od Umowy odstąpić jeszcze przed upływem terminu wykonania Umowy
3. Zamawiający może odstąpić od Umowy, z przyczyn leżących po stronie Wykonawcy, w przypadku:
    1) złożenia wniosku o ogłoszenie upadłości lub otwarcia likwidacji Wykonawcy,
    2) zmiany formy organizacyjnej Wykonawcy, utrudniającej wykonanie Umowy, pod warunkiem, że nowy Wykonawca nie spełnia warunków udziału w postępowaniu, zachodzą wobec niego podstawy wykluczenia oraz pociąga to za sobą inne istotne zmiany Umowy - w ciągu 14 dni od dnia powzięcia wiadomości o takiej okoliczności.
4. Zamawiający może odstąpić od Umowy w przypadku zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, w ciągu 30 dni od dnia powzięcia wiadomości o tej okoliczności.
5. W przypadku odstąpienia od Umowy określonego w ust. 3 i 4 Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu faktycznego wykonania części Umowy.
6. Odstąpienie od Umowy następuje w formie pisemnej pod rygorem nieważności, ze wskazaniem przyczyny odstąpienia.
7. Skorzystanie z prawa odstąpienia od Umowy nie znosi odpowiedzialności z tytułu zastrzeżonych w niej kar umownych i nie wyłącza uprawnienia do ich dochodzenia.

§ 10

Przetwarzanie danych osobowych

1. Zamawiający oświadcza, że będzie przetwarzał dane osobowe przekazane przez Wykonawcę w związku z realizacją przedmiotu umowy oraz, że posiada wdrożone odpowiednie środki techniczne i organizacyjne wymagane na mocy art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz przepisów ustawy o ochronie danych osobowych.
2. Zamawiający informuje, że zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz. Urz. UE L 119/1:

    1) administratorem danych osobowych osób reprezentujących Wykonawcę jest Minister Sprawiedliwości z siedzibą w Warszawie, Al. Ujazdowskie 11,

    2) dane osobowe osób, o których mowa w punkcie 1, to w szczególności: imię i nazwisko, dane kontaktowe,

    3) kontakt z Inspektorem Ochrony Danych – Tomasz Osmólski, tel. 22 23 90 642, e-mail: iod@ms.gov.pl,

4) dane osobowe osób, o których mowa w punkcie 1, przetwarzane będą w celu realizacji umowy - na podstawie art. 6 ust. 1 lit. b ogólnego rozporządzenia o ochronie danych,

5) odbiorcami danych osobowych osób, o których mowa w punkcie 1, będą: - organy kontrolne i nadzorcze oraz audyt, w tym ZUS, US,

6) dane osobowe osób, o których mowa w punkcie 1, przechowywane będą zgodnie z postanowieniami instrukcji kancelaryjnej Ministerstwa Sprawiedliwości, tj. wynikające z umowy cywilnoprawnej bez ZUS - lat 5, a z umowy cywilnoprawnej z ZUS - lat 50,

7) osoby, o których mowa w punkcie 1, posiadają prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania,

8) osoby, o których mowa w punkcie 1, mają prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych (adres: ul. Stawki 2, 00-193 Warszawa),

2. W stosunku do danych osobowych przekazanych Wykonawcy przez Zamawiającego, Wykonawca oświadcza, że:
   1) będzie przetwarzał dane osobowe przekazane przez Zamawiającego tylko w celach związanych z realizacją przedmiotu umowy na podstawie art. 6 ust. 1 lit. b ogólnego rozporządzenia o ochronie danych,
2) administratorem danych osobowych osób reprezentujących Zamawiającego jest …….
3) dane osobowe osób, o których mowa w pkt 1, to w szczególności: imię i nazwisko, dane kontaktowe,
4) osoby, o których mowa w punkcie 1, posiadają prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania,
5) osoby, o których mowa w punkcie 1, mają prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych (adres: ul. Stawki 2, 00-193 Warszawa).

§ 11

Postanowienia końcowe

1. Prawem właściwym dla Umowy jest prawo polskie.
2. Żadna ze Stron Umowy nie może przenieść praw i obowiązków wynikających z niniejszej Umowy na osobę trzecią bez uprzedniego uzyskania zgody drugiej Strony, wyrażonej w formie pisemnej pod rygorem nieważności.
3. Sądem właściwym do rozstrzygnięcia sporów wynikłych z realizacji postanowień niniejszej Umowy będzie sąd miejscowo właściwy dla siedziby Zamawiającego.
4. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, w tym dwa egzemplarze dla Zamawiającego i jeden dla Wykonawcy.

Załączniki:

Załącznik nr 1 – Opis Przedmiotu Zamówienia

Załącznik nr 2 – Wzór Protokołu odbioru szkolenia

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1 do umowy nr … z dnia ……

Opis przedmiotu zamówienia

I. Przedmiot zamówienia:

Przeprowadzenie szkolenia z zakresu egzaminu Certified Information Systems Security Professional.

II. Termin wykonania zamówienia:

Od dnia zawarcia umowy do dnia 31 października 2021 roku.

III. Zakres i wymagania szczegółowe Certified Information Systems Security Professional (CISSP)

1. Szkolenia zostaną przeprowadzone na terenie Warszawy. Wykonawca zobowiązany jest do przeprowadzenia szkolenia do 31 października 2021 roku.
2. W szkoleniu uczestniczyć będzie jeden pracownik Zamawiającego.
3. Uczestnik otrzyma dokument poświadczający ukończenie szkolenia.
4. Szkolenia muszą zostać przeprowadzone w języku polskim lub angielskim.
5. Wykonawca zobowiązuje się do zaproponowania co najmniej dwóch terminów szkolenia do wyboru przez Zamawiającego.
6. Zakres merytoryczny szkolenia przygotowującego do egzaminu CISSP CAT musi obejmować wszystkie tematy wyszczególnione w dokumencie „CISSP Exam Outline", dostępnym na oficjalnej stronie (ISC)², to jest:
    a. security and risk management:
        i. understand and apply security governance principles: alignment of security function to business strategy, goals, mission and objectives; organizational processes (e. g. acquisitions, divestitures, governance comittiees), organizational roles and responsibilites; security control frameworks; due care/due diligience,
        ii. determine compliance requirements: contractual, legal, industry standards, and regulatory requirements; privacy requirements;
        iii. understand legal and regulatory issues that pertain to information security in global context: cyber crimes and data breaches; licensing and intellectual property requirements; import/export controls; trans-border data flow; privacy;
        iv. understand, adhere to and promote professional ethics: (ISC)^2 code of professional ethics; organizational code of ethics;
        v. develop, document and implement security policy standards, procedures and guidelines,
        vi. identify, analyze and proritize business continuity (BC) requirements: develop and document scope and plan; business impact analysis (BIA);
        vii. contribute to and enforce personnel security policies and procedures: candidate screening and hiring; employment agreements and policies; onboarding and termination processes; vendor, consultant and contractor agreement and controls; compliance policy requirements; privacy policy requirements;
        viii. understand and apply risk management concepts: identify threats and vulnerabilities; risk assessment/analysis; risk response; countermeasures selection and implementation; applicable types of controls (e. g., preventive, detective, corrective); security control assessment (SCA);

monitoring and measurement; asses valuation; reporting; continuous improvement; risk frameworks;

ix. understand and apply threat modeling concepts and methodologies: threat modeling methodologies; threat modeling concepts;
x. apply risk-based management concepts to the supply chain: risk associated with hardware, software and services; third-party assessment and monitoring; minimum security requirements; service-level requirements;
xi. establish and maintain a security awareness, education and training program: methods and techniques to present awareness and training; periodic content reviews; program effectiveness evaluation;

b. asset security:
    i. identify and classify information and assets: data classification, asset classification;
    ii. determine and maintain information and asset ownership;
    iii. protect privacy: data owners; data processers; data remanence; collection limitation;
    iv. ensure appropriate asset retention;
    v. determine data security controls: understand data states; scoping and tailoring; standards selection; data protection methods;
    vi. establish information and asset handling requirements;
c. security architecture and engineering:
    i. implement and manage engineering processes using secure design principles;
    ii. understand the fundamental concepts of security models;
    iii. select controls based upon systems security requirements;
    iv. understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption);
    v. assess and mitigate the vulnerabilities of security architectures, designs and solution elements: client-based systems; server-based systems; database systems; cryptographic systems; industrial control systems (ICS); cloud-based systems; distributed systems; internet of things (IoT);
    vi. assess and mitigate vulnerabilities in web-based systems;
    vii. assess and mitigate vulnerabitilies in mobile systems;
    viii. assess and mitigate vulnerabilities in embedded devices;
    ix. apply cryptography: cryptographic life cycle (e.g., key management, algorithm selection); cryptographic methods (e.g., symmetric, asymmetric, elliptic curves); Public Key Infrastructure (PKI); key management practices; digital signatures; non-repudiation; integrity (e.g., hashing); understand methods of cryptoanalytic attacks; digital rights management (DRM);
    x. apply security principles to site and facility design;
    xi. implement site and facility security console controls: wiriting closets/intermediate distribution facilities; server rooms/data centers; media storage facilities; evidence storage; restricted and work area security; utilities and heating, ventilation, and air conditioning (HVAC); environmental issues; fire prevention, detection and suppression;
d. communication and network security:
    i. open system interconnection (OSI) and transmission control protocol/internet protocol (TCP/IP) models; internet protocol (IP)

networking; implications of multilayer protocols; converged protocols; software-defined networks; wireless networks;

ii. secure network components: operation of hardware; transmission media; network access control (NAC); endpoint security; content-distribution networks;

iii. implement secure communication channels according to design: voice; multimedia collaboration; remote access; data communications; virtualized networks;

e. identity and access management (IAM):

i. control physical and logical access to assets: information, systems, devices, facilities;

ii. manage identification and authentication of people, devices and services: identity management implementation, single/multi-factor authentication; accountabilitiy; session management; registration and proofing of identity; federated identity management (FIM); credential management systems;

iii. integrate identity as a third-party service: on-premise; cloud; federated;

iv. implement and manage authorization mechanisms: role based access control (RBAC); rule-based access control, mandatory access control (MAC); discretionary access control (DAC); attribute based access control (ABAC);

v. manage the identity and access provisioning cycle: user access review; system account access review; provisioning and deprovisioning;

f. security assessment and testing:

i. design and validate assessment, test, and audit strategies: internal; external; third-party;

ii. conduct security control testing: vulnerability assessment; penetration testing; log reviews; synthetic transactions; code review and testing; misuse case testing; test coverage analysis; interface testing;

iii. collect security process data (e.g., technical and administrative): account management; management review and approval; key performacne and risk indicators; backup verification data; training and awareness; disaster recovery (DR) and business continuity (BC);

iv. analyze test output and generate report;

v. conduct or facilitate security audits: internal; external; third-party;

g. security operations:

i. understand and support investigations: evidence collection and handling; reporting and documentation; investigate techniques; digital forensics tools, tactics, and procedures;

ii. understand requirements for investigation types: administrative; criminal; civil; regulatory; industry standards;

iii. conduct logging and monitoring activities: intrusion detection and prevention; security information and event management (SIEM); continuous monitoring; egress monitoring;

iv. securely provisioning resources: asset inventory; asset management; configuration management;

v. understand and apply founfdational security operations concepts: need-to-know/least privileges; separation of duties and responsibilities; privileged account management; job rotation; information lifecycle; service level agreements (SLA);

vi. apply resource protection techniques: media management; hardware and software asset management;
vii. conduct incident management: detection; response; mitigation; reporting; recovery; remediation; lessons learned;
viii. operate and maintaing detective and preventative measures: firewall;s intrusion detection and prevention systems; whitelisting/blacklisting; third-party provided security services; sandboxing; honeypots/honeynets; anti-malware;
ix. implement and support patch and vulnerability management;
x. understand and participate in change management processes;
xi. implement recovery strategies: backup storage strategies; recovery site strategies; multiple processing sites; system resilience, high availability, quality of service (QoS), and fault tolerance;
xii. implement disaster recovery (DR) processes: response; personnel; communications; assessment; restoration; training and awareness;
xiii. test disaster recovery plans (DRP): read-through/tabletop; walkthrough; simulation; parallel; full interruption;
xiv. participate in business continuity (BC) planning and exercises;
xv. implement and manage physical security: perimeter security controls; internal security controls;
xvi. address personnel safety and security concerns: travel; security and training awareness; emergency management; duress;

h. software development security:
i. understand and integrate security in the software development life cycle (SDLC): development methodologies; maturity models; operation and maintenance; change management; integrated product team;
ii. identify and apply security controls in development environments: security of the software evnironments; configuration management as an aspect of secure coding; security of code repositories;
iii. assess the effectiveness of software security: auditing and logging of changes; risk and analysis mitigation;
iv. assess security impact of acquired software;
v. define and apply secure coding guidelines and standards: security weaknesses and vulnerabilities at the source-code level; security of application programming interfaces; secure coding practices;

7. Podmiot przeprowadzający szkolenie musi posiadać autoryzację (ISC)2 do przeprowadzania oficjalnych szkoleń przygotowujących do egzaminu CISSP.

IV. Warunki przeprowadzania szkoleń

1. Wykonawca, przygotuje harmonogram szkolenia oraz program szkolenia i dostarczy je w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji przez Zamawiającego. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego szkolenia.
2. Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika szkolenia, pozwalające na samodzielną edukację z zakresu tematyki szkolenia (np. opracowania, wydruki materiałów szkoleniowych).

3. Komplet materiałów szkoleniowych dla uczestnika szkolenia obejmuje papierową wersję materiałów szkoleniowych. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych.
4. Wykonawca dostarczy uczestnikowi szkolenia ww. materiały szkoleniowe najpóźniej w dniu rozpoczęcia szkolenia..
5. Koszty opracowania, powielenia i transportu materiałów szkoleniowych ponosi Wykonawca.
6. Zamawiający dopuszcza przeprowadzenie szkolenia z wykorzystaniem narzędzi umożliwiających wideokonferencję na poniższych warunkach:
    a. Oprogramowanie wykorzystane do udostępnienia ekranu komputera prowadzącego, obrazu oraz dźwięku z sali szkoleniowej zostanie udostępnione uczestnikom szkolenia bez ponoszenia przez Zamawiającego dodatkowych kosztów. Wykorzystane oprogramowanie będzie pochodzić z legalnego źródła oraz sposób użycia nie może naruszać warunków licencyjnych, na jakich oprogramowanie zostało udostępnione.
    b. Wykorzystane oprogramowanie musi umożliwiać uczestnikom szkolenia zadawanie pytań i zgłaszanie wątpliwości w czasie rzeczywistym.
    c. Sposób prowadzenia szkolenia przez prowadzącego musi umożliwiać uczestnikom zadawanie pytań i zgłaszanie wątpliwości w czasie rzeczywistym.

Załącznik nr 2 do umowy nr … z dnia ……

Protokół odbioru szkolenia

Warszawa, dnia ……

Protokół z przeprowadzonego szkolenia Certified Information Systems Security Professional

W dniach …… - …… odbyło się szkolenie z zakresu egzaminu Certified Information Systems Security Professional.

Plan szkolenia:

1. Dnia …:
    a. …
    b. …
    c. etc.
2. Dnia …:
    a. …
    b. …
    c. etc.
3. etc.

W szkoleniu udział wzięli:

1. Dnia …:
    a. …
    b. …
    c. etc.
2. Dnia …:
    a. …
    b. …
    c. etc.
3. etc.

…… ……

podpis osoby przeprowadzającej szkolenie podpis osoby odbierającej szkolenie