**Istotne postanowienia umowy (IPU)**

**§ 1**

**Przedmiot Umowy**

1. W ramach Umowy, Wykonawca zobowiązuje się na rzecz Zamawiającego do:
   1. przeprowadzenia szkolenia przygotowującego do egzaminu CompTIA Security+ SY0-501 dla czterech osób,
   2. przeprowadzenia egzaminu certyfikacyjnego CompTIA Security+ SY0-501 dla czterech osób.
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 i egzaminu do wyboru Zamawiającego.
2. Wykonawca zobowiązuje się do przeprowadzenia szkolenia w terminie nie później niż do 20 grudnia 2019 roku.
3. Wykonawca zobowiązuje się do przeprowadzenia egzaminu nie wcześniej niż 2 miesiące i nie później niż 6 miesięcy licząc od dnia zakończenia szkolenia.
4. Przeprowadzenie szkolenia i egzaminu zostanie potwierdzone odpowiednim protokołem, podpisanym przez Zamawiającego, w terminie do 7 dni od dnia zakończenia szkolenia lub egzaminu, zgodnie ze wzorami stanowiącymi Załącznik nr 2 i nr 3 do Umowy.

**§ 3**

**Wynagrodzenie oraz warunki płatności**

1. Za wykonanie całego przedmiotu umowy, Zamawiający zapłaci Wykonawcy wynagrodzenie w wysokości …………………… zł brutto/netto\* (słownie: …………………………………………), w tym:
2. za przeprowadzenie szkolenia dla 4 osób w wysokości: ………….. zł brutto/netto\* (słownie: ………….),
3. za przeprowadzenie egzaminu dla 4 osób w wysokości: ………………… zł brutto/netto\* (słownie: …………..).

\*niepotrzebne skreślić

1. 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 i egzaminu, zgodnie z wyszczególnionymi w Opisie Przedmiotu Zamówienia wytycznymi.
2. Wynagrodzenie płatne będzie po przeprowadzeniu szkolenia w wysokości określonej w ust. 1 pkt 1 oraz po przeprowadzeniu egzaminu w wysokości określonej w ust. 1 pkt 2.
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 ……………………. .

1. Ze strony Wykonawcy, osobą odpowiedzialną za realizację Umowy oraz upoważnionymi do kontaktów jest:

- …………………… tel. ……………………, e-mail ……………………. .

1. 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. 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,
   2. w razie opóźnienia w wykonaniu przedmiotu umowy w terminie określonym w § 2 ust. 2 lub w §2 ust. 3 - w wysokości 0,5% całkowitego wynagrodzenia brutto określonego w § 3 ust. 1 za każdy dzień opóźnienia,
   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.

1. 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.
2. 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.
3. Wykonawca nie może powierzyć przetwarzania informacji innym podmiotom bez uprzedniego uzyskania w tym przedmiocie pisemnej zgody Zamawiającego.
4. W przypadku powierzenia przez Wykonawcę informacji, Wykonawca odpowiada za działania i zaniechania tych podmiotów, jak za własne działania lub zaniechania.
5. 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.
6. 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 dniod 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**

**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

Załącznik nr 3 – Wzór Protokołu odbioru egzaminu

**ZAMAWIAJĄCY WYKONAWCA**

Załącznik nr 1 do umowy nr … z dnia …………

**Opis przedmiotu zamówienia**

**I. Przedmiot zamówienia:**

Przeprowadzenie szkoleń z zakresu egzaminu CompTIA Security+ (SY0-501) oraz organizacja egzaminu certyfikacyjnego.

**II. Termin wykonania zamówienia:**

Od dnia zawarcia umowy do dnia 20. grudnia 2019 roku.

**III. Zakres i wymagania szczegółowe CompTIA Security+ (SY0-501):**

1. Szkolenia i egzamin zostaną przeprowadzone na terenie Warszawy. Wykonawca zobowiązany jest do przeprowadzenia szkoleń do 20. grudnia 2019 roku, a egzaminów w terminie do sześciu miesięcy od momentu podpisania umowy.
2. W szkoleniu i egzaminach uczestniczyć będzie czterech pracowników Zamawiającego.
3. Każdy uczestnik otrzyma dokument poświadczający ukończenie szkolenia.
4. Szkolenia i egzaminy muszą zostać przeprowadzone w języku polskim lub angielskim.
5. Wykonawca zobowiązuje się do zaproponowania co najmniej jednego terminu szkolenia do wyboru przez Zamawiającego.
6. Zakres merytoryczny szkolenia przygotowującego do egzaminu SY0-501 musi obejmować wszystkie tematy wyszczególnione w dokumencie „CompTIA Security+ Certification Exam Objectives”, dostępnym na oficjalnej stronie CompTIA, to jest:
   1. 1.1 – viruses, crypto-malware, ransomware, worm, trojan, rootkit, keylogger, adware, spyware, bots, RAT, logic bomb, backdoor;
   2. 1.2 – social engineering: phishing, spear phishing, whaling, vishing, tailgating, impersonation, dumpster diving, shoulder surfing, hoax, watering hole attack; principles: authority, intimidation, consensus, scarcity, familiarity, trust, urgency; apllication/service attacks: DoS, DDoS, man-in-the-middle, buffer overflow, injection, cross-site scripting, cross-site request forgery, privilege escalation, ARP poisoning, amplification, DNS poisoning, domain hijacking, man-in-the-browser, zero day, replay, pass the hash; hijacking and related attacks: clickjacking, session hijacking, url hijackng, typo squatting; driver manipulation: shimming, refactoring; MAC spoofing, IP spoofing; wireless attacks: replay, IV, evil twin, rogue AP, jamming, WPS, bluejacking, bluesnarfing, RFID, NFC, disassociation; cryptographic attacks: birthday, known plain text/cipher text, rainbow tables, dictionary, brute force: online vs. offline, collision, downgrade, replay, weak implementations;
   3. 1.3 – explain threat actor types and attributes; types of actors: script kiddies, hacktivist, organized crime, nation states/APT, insiders, competitors; attributes of actors: internal/external, level of sophistication, resources/funding, intent/motivation; use of open-source intelligence;
   4. 1.4 – explain penetration testing concepts; active reconnaissance, passive reconnaisance, pivot, initial exploitation, persistence, escalation of privilege, black box, white box, gray box, penetration testing vs. vulnerability scanning;
   5. 1.5 – explain vulnerability scanning concepts; passively test security controls, identify vulnerability, identfiy lack of security controls, identify common misconfigurations, intrusive vs. non-instrusive, credentialed vs. non-credentialed, false positive;
   6. 1.6 – explain the impact associated with types of vulnerabilities; race conditions; vulnerabilities due to: end-of-life systems, embedded systems, lack of vendor suport, improper input handling, improper error handling, misconfiguration/weak configuration, default configuration, resource exhaustion, untrained users, improperly configured accounts, vulnerable business proces, weak cipher suites and implementations; memory/buffer vulnerability: memory leak, integer overflow, buffer overflow, pointer dereference, DLL injection; system sprawl/undocumented assets, architecture/design weaknesses, new threats/zero day, improper certificate and key management;
   7. 2.1 install and configure network components, both hardware- and software-based, to suport organizational security; firewall: ACL, application-based vs. network-based, stateful vs. stateless, implicit denny; VPN concentrator: remote access vs. site-to-site, IPsec: tunel mode, transport mode, AH, ESP; split tunnel vs. full tunnel, TSL, always-on VP?N; NIPS/NIDS: signature-based, heuristic/behavioral, anomaly, inline vs. passive, in-band vs. out-of-band, rules, analytics: false positive, false negative; router: ACLs, antispoofing; switch: port security, layer 2 vs. layer 3, loop prevention, flood guard; proxy: forward and reverse proxy, transparent, application/multipurpose; load balancer; scheduling: affinity, round-robin, active-passive, active-active, virtual IPs; access point: SSID, MAC filtering, signal strenght, band selection/width, antenna types and placement, fat vs. thin, controller based vs. standalone; SIEM: aggregation, correlation, automated alerting and triggers, time synchronization, event deduplication, Logs/WORM; DLP: usb blocking, cloud-based, email; NAC: dissolvable vs. permanent, host health checks, agent vs. agentless; mail Gateway: spam filter, DLP, encryption; bridge, SSL/TLS accelerators, SSL decryptors, media gateway, hardware security module;
   8. 2.2 – given a scenario, use appropriate software tools to assess the security posture of an organization; protocol analyzer, network scanners: rogue system detection, network mapping; wireless scanners/cracker, password cracker, vulnerability scanner, configuration compliance scanner, exploitation frameworks, data sanitization tools, steganography tools, honeypot, backup utilities, banner grabbing, passive vs. active, command line tools: ping, netsat, tracert, nslookup/dig, arp, ipconfig/ip/ifconfig, tcpdump, nmap, netcat;
   9. 2.3 – given a scenario, troubleshoot common security issues; unecrypted credentials/clear text, logs and events anomalies, permission issues, access violations, certificate issues, data exfiltration, misconfigured devices: firewall, content filter, access points; weak security configurations, personnel issues: policy violation, insider threat, social engineering, social media, personal email; unathorized software, baseline deviation, license compliance violation (availability/integrity), asset management, authentication issues;
   10. 2.4 – given a scenario, analyze and interpret otuput from security technologies; HIDS/HIPS, antivirus, file integrity check, host-based firewall, application whitelisting, removable media control, advanced malware tools, UTM, DLP, data execution prevention, web application firewall;
   11. 2.5 – given a scenario, deploy mobile devices securely; connection methods: cellular, WiFi, SATCOM, Bluetooth, NFC, ANT, Infrared, USB; mobile device management concepts: application management, content management, remote wipe, geofencing, geolocation, screen locks, push notification services, password and pins, biometrics, content-aware authentication, conainterization, storage segmentation, full device encryption; enforcement and monitoring for: third-party app stores, rooting/jailbreaking, sideloading, custom firmware, carrier unlocking, firmware OTA updates, camera use, SMS/MMS, external media, USB OTG, recording microphone, GPS tagging, WiFi direct/adhoc, tethering, payment methods; deploment models: BYOD, COPE, CYOD, corporate-owned, VDI;
   12. 2.6 – given a scenario, implement secure protocols; protocols: DNSSEC, SSH, S/MIME, SRTP, LDAPS, FTPS, SFTP, SNMPV3, SSL/TLS, HTTPS, seucre POP/IMAP; use cases: voice and video, time synchronization, email and web, file transfer, directiory services, remote access, domain name and resolution, routing and switching, network address allocation, subscription services;
   13. 3.1 – explain use cases and purpose for frameworks, best practices and secure configuration guides; industry-standard frameworks and reference architectures: regulatory, non-regulatory, national vs. international, industry-specific frameworks; benchmarks/secure configuration guides: platform/vendor-specific guides: web server, application server, network infrastructure devices; general purpose guides; defense-in-depth/layered security: vendor diversity, control diversity (administrative/technical), user training;
   14. 3.2 – given a scenario, implement secure network architecture concepts; zones/topologies: dmz, extranet, intranet, wireless, guest, honeynets, NAT, ad-hoc; segregation/segmentation/isolation: physical, logical (VLAN), virtualization, air gaps; tunneling/VPN: site-to-site, remote access; security device/technology placement: sensors, collectors, correlation engines, filters, proxies, firewalls, VPN concentrators, SSL accelerators, load balancers, DDoS mitigator, aggregation switches, taps and port mirror; SDN;
   15. 3.3 – given a scenario, implement secure systems desing; hardware/firmware security: FDE/SED, TPM, HSM, UEFI/BIOS, secure boot and attestation, supply chain, hardware root of trust, EMI/EMP; operating systems: types (network, serwer, workstation, appliance, kiosk, mobile OS); patch management, disabling unnecessary ports and services, least functionality, secure configurations, trusted operating system, application whitelisting/blacklisting, disable default accounts/passwords; peripherals: wireless keyboards, wireless mice, displays, WiFi-enabled MicroSD cards, printers/MFDs, external storage devices, digital cameras;
   16. 3.4 – explain the importance of secure staging deployment concepts; sandboxing, environment: development, test, staging, production; secure baseline, integrity measurement;
   17. 3.5 – explain the security implications of embedded systems; SCADA/ICS, smart devices/IoT: wearable technology, home authentication; HVAC, SoC, RTOS, printers/MFDs, camera systems, special purpose: medical devices, vehicles, aircraft/UAV;
   18. 3.6 – summarize secure application development and deployment concepts; development life-cycle models: waterfall vs. agile; secure DevOps: security automation, continuous integration, baselining, immutable systems, infrastructure as code; version control and change management, provisioning and deprovisioning, secure coding techniques: proper error handling, proper input validation, normalization, stored procedures, code signing, encryption, obfuscating/camouflage, code reuse/dead code, server-side vs. client-side execution and validation, memory management, use of third-party libraries and SDKs, data exposure; code quality and testing: static code analyzers, dynamic analysis (e.g., fuzzing), stress testing, sandboxing, model verification; compiled vs. runtime code;
   19. Summarize cloud and virtualization concepts; hypervisor: type I, type II, application cells/cointainters; VM sprawl avoidance, VM escape protection, cloud storage, cloud deployment models: SaaS, PaaS, IaaS, private, public, hybrid, community; on-premise vs. hosted vs. cloud, VDI/VDE, cloud access security broker, securty as a service;
   20. 3.8 – explain how resiliency and automation strategies reduce risk; automation/scripting: automated courses of action, continuous monitoring, configuration validation; templates, master image, non-persistence: snapshots, revert to known state, rollback to known configuration, live boot media; elasticity, scalability, distributive allocation, redundancy, fault tolerance, high availability, RAID;
   21. 3.9 – explain the importance of physical security controls; lighting, signs, fencing/gate/cage, security guards, alarms, safe, secure cabinets/enclosures, protected distribution/protected cabling, airgap, mantrap, faraday cage, lock types, biometrics, barricades/bollards, tokens/cards, environmental controls: HVAC, hot and cold aisles, fire suppression; cable locks, screen filters, cameras, motion detection, logs, infrared detection, key management;
   22. 4.1 – compare and contrast identity and access management concepts; identification, authentication, authorization and accounting (AAA); multifactor authentication: something you are/have/know, somewhere you are, something you do; federation, single sign-on, transitive trust;
   23. 4.2 – given a scenario, install and configure identity and access services; LDAP, Kerberos, TACACS+, CHAP, PAP, MSCHAP, RADIUS, SAML, OpenID Connect, OAUTH, Shibboleth, Secure token, NTLM;
   24. 4.3 – given a scenario, implement identity and access management controls; access control models: MAC, DAC, ABAC, role-based access control, rule-based access control; physical access control: proximity cards, smart cards; Biometric factors: fingerprint/retinal/iris scanner, voice/facial recognition, false acceptance rate, false rejection rate, crossover error rate; tokens: hardware, software, HOTP/TOTP; certificate-based authentication: PIV/CAC/smart card, IEEE 802.1X; file system security, database security;
   25. 4.4 – given a scenario, differentiate common account management practices; account types: user account, ashared and generic accounts/credentials, guest accounts, service accounts, privileged accounts; general concepts: least privilege, onboarding/offboarding, permission auditing and review, usage auditing and review, time-of-day restrictions, recertification, standard naming convention, account maintenance, group-based access control, location-based policies; account policy enforcement: credential management, group policy, password complexity, expiration, recovery, diablement, lockout, password history/reuse/lenght;
   26. 5.1 – explain the importance of policies, plans and procedures related to organization security; standard operating procedurę, agreement types: BPA, SLA, ISA, MOU/MOA; personnal management: mandatory vacations, job rotation, separation of duties, clean desk, background checks, exit interviews, role-based awareness training: data owner, system administrator, system owner, user, privileged user, executive user, NBA, onboarding, continuing education, acceptable use policy/rules of behawior, adverse actions; general security policies: social media networks/applications, personal email;
   27. 5.2 – summarize business impact analysis concepts; RTO/RPO, MTBF, MTTR, mission-essential functions, identification of critical systems, single point of failure, impact: life, property, safety, finance, reputation; privacy impact assessment, privacy threshold assessment;
   28. 5.3 – explain risk management processes and concepts; threat assessment: environmental, manmade, internal vs. external, risk assesment SLE, ALE, ARO, asset-value, risk register, likehood of occurrence, supply chain assessment, impact, quantitative, qualitative, testing: penetration testing authorization, vulnerability testing authorization; risk response techniques: accept, transfer, avoid, mitigate; change management;
   29. 5.4 – given a scenario, follow incident response procedures; incident reponse plan: documented incident types/category definitions, roles and responsibilities, reporting requirements/escalation, cyber-incident response teams, exercise; incident reposnse proces: preparation, identification, containment, eradication, recovery, lessons learned;
   30. 5.5 – summarize basic concepts of forensics; order of volatility, chain of custody, legal hold, data acquisition: capture system image, network traffic and logs, capture video, record time offset, take hashes, screenshots, witness interviews; preservation, recovery, strategic intelligence/counterintelligence gathering: active logging; track man-hours;
   31. 5.6 – explain disaster recovery and continuity of operation concepts; recovery sites: hot site, warm site, cold site; order of restoration; backup concepts: differentia, incremental, snapshots, full; geographic considerations: off-site backups, distance, location selection, legal implications, data sovereignity; continuity of operation planning: exercises/tabletop, after-action reports, failover, alternate processing sites, alternate business practices;
   32. 5.7 – compare and contrast various types of controls; deterrent, preventive, detective, corrective, compensating, technical, administrative, physical;
   33. 5.8 – given a scenario, carry out data security and privacy practices; data destruction and media sanitization: burning, shredding, pulping, pulverizing, degaussing, purging, wiping; data sensivity labeling and handling: confidential, private, public, proprietary, PII, PHI; data roles: owner, steward/custodian, privacy oficer; data retention, legal and compliance;
   34. 6.1 – compare and contrast basic concepts of cryptography; symmetric algorithms, modes of operation, assymetric algorithms, hashing, salt, IV, nonce, elliptic curve, weak/deprecated algorithms, key exchange, digital signatures, diffusion, confusion, collision, steganography, obfuscation, stream vs. block, key strength, session keys, ephemeral key, secret algorithm, data-in-transit, data-at-rest, data-at-use, random/pseudo-random number generation, key stretching, implementation vs. algorithm selection: crypto service provider, crypto modules; perfect forward secrecy, security through obscurity, common use cases: low power devices, low latency, high resiliency, suporting confidentiality/integrity/obfuscation/authentication/non-repudiation, resource vs. security constraints;
   35. 6.2 – explain cryptography algorithms and their basic characteristics; symmetric algorithms: AES, DES, 3DES, RC4, blowfish/twofish; cipher modes: CBC, GCM, ECB, CTR, stream vs. block; assymetric algorithms: RSA, DSA, Diffie-Hellman (groups, DHE, ECDHE), elliptic curve, PGP/GPG; hashing algorithms: MD5, SHA, HMAC, RIPEMD; key strerching algorithms: BCRYPT, PBKDF2; obfuscation: XOR, ROT13, substitution ciphers;
   36. 6.3 – given a scenario, install and configure wireless security settings; cryptographic protocols: WPA, WPA2, CCMP, TKIP; authentication protocols: EAP, PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, IEEE 802.1X, RADIUS Federation; methods: PSK vs. enterprise vs. open, WPS, captive portals;
   37. 6.4 – given a scenario, implement public key infrastructure; components: CA, intermediate CA, CR, OCSP, CSR, certificate, public key, private key, object identifiers (OID); concepts: online vs. offline CA, stapling, pinning, trust model, key escrow, certificate changing; types of certificates: wildcard, SAN, code signing, self-signed, machine/computer, email, user, root, domain validation, extended validation; certificate formats: DER, PEM, PFX, CER, P12, P7B.
7. Podmiot przeprowadzający szkolenie przygotowujące do egzaminu SY0-501 musi posiadać status autoryzowanego przez CompTIA partnera szkoleniowego w zakresie przygotowania do egzaminu CompTIA Security+ (SY0-501).

**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 każdego 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 uczestnikom szkolenia ww. materiały szkoleniowe najpóźniej w dniu rozpoczęcia szkolenia.
5. Koszty opracowania, powielenia i transportu materiałów szkoleniowych ponosi Wykonawca.
6. Wykonawca dla uczestników szkolenia zapewni wyżywienie, o którym mowa w ust. 7. Posiłki serwowane będą w odpowiednim pomieszczeniu, wyposażonym w niezbędną liczbę stołów i krzeseł. Zamawiający nie dopuszcza serwowania posiłków w tej samej sali, w której odbywają się szkolenia. Miejsce posiłku nie powinno być oddalone dalej niż 10 minut drogi pieszo od miejsca szkolenia; obiady powinny być zróżnicowane, dany zestaw obiadowy nie powinien powtarzać się częściej niż raz na 3 dni szkoleniowe; Wykonawca zapewni co najmniej 2 przerwy kawowe podczas jednego dnia szkoleniowego.
7. W zakresie wyżywienia uczestników szkolenia, Wykonawca zapewni:
   * 1. obiad dla wszystkich uczestników szkolenia. Zestaw obiadowy obejmuje co najmniej: zupę, gorące danie główne (rybne lub mięsne) z dodatkami skrobiowymi oraz surówką lub sałatkami; kawę i herbatę wraz z dodatkami (co najmniej cukier, mleczko do kawy, cytryna); wodę mineralną gazowaną i niegazowaną;
     2. serwis kawowy, na który składać się będą: woda gazowana i niegazowana w butelkach, herbata, kawa parzona z zaparzacza lub ekspresu, dodatki (cukier, mleko do kawy, cytryna) i dodatki np. ciastka/wafelki/ciasto/inne słodycze.
8. Wykonawca zobowiązany jest do:
   * 1. terminowego przygotowania i podania posiłków, zgodnie z ramowym programem szkolenia,
     2. zachowania zasad higieny i obowiązujących przepisów przy przygotowaniu posiłków i ich podawaniu,
     3. przygotowania posiłków zgodnie z zasadami racjonalnego wyżywienia, urozmaiconych z pełnowartościowych, świeżych produktów z ważnymi terminami przydatności do spożycia,
     4. przestrzegania w trakcie realizacji usług wchodzących w zakres przedmiotu umowy obowiązujących przepisów sanitarnych, w tym ustawy z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia. (**Dz.U. z 2019 r. poz. 1252**).
9. Czas na przerwy kawowe i obiadowe należy doliczyć do założonej liczby godzin szkolenia.
10. Koszty posiłków, dowozu, sprzętu i obsługi ponosi Wykonawca.

**V. Warunki i wymagania dotyczące przeprowadzania egzaminów**

1. Wykonawca zapewni na cele realizacji przedmiotu zamówienia bazę egzaminacyjną z odpowiednimi pomieszczeniami wraz z zapleczem do przeprowadzenia egzaminów dla osób dorosłych, tj. sale dostosowane do przeprowadzania egzaminów, dobrze oświetlone (światło dzienne i sztuczne), wentylowane (z dostępem do świeżego powietrza), posiadające odpowiednie warunki sanitarne, bezpieczeństwa i higieny pracy, wyposażone w akustyczne i jakościowe narzędzia i urządzenia, a także oprogramowanie i pomoce dydaktyczne niezbędne do wykonania zamówienia.
2. W pobliżu sali egzaminacyjnej (w tym samym budynku) powinny znajdować się łazienki z węzłem sanitarnym.
3. Egzamin zostanie przeprowadzony nie wcześniej niż 2 miesiące i nie później niż 6 miesięcy po zakończeniu szkolenia.
4. Egzamin odbędzie się w dzień powszedni od poniedziałku do piątku, w godzinach od 8:00 do 17:00.
5. Egzamin zostanie przeprowadzony na terenie Warszawy.
6. Do egzaminu przystąpi czterech pracowników Zamawiającego, którzy ukończyli szkolenie.
7. Każdy uczestnik otrzyma dokument potwierdzający przystąpienie do egzaminu wraz z jego wynikami.
8. Egzamin będzie przeprowadzony w języku polskim lub angielskim.
9. Wykonawca zobowiązuje się do wskazania trzech terminów egzaminu do wyboru przez Zamawiającego.
10. Podmiot przeprowadzający egzamin CompTIA Security+ (SY0-501) musi posiadać status podmiotu egzaminującego autoryzowanego przez CompTIA.

Załącznik nr 2 do umowy nr … z dnia …………

**Protokół odbioru szkolenia**

Warszawa, dnia …………

Protokół z przeprowadzonego szkolenia CompTIA Security+ (SY0-501)

W dniach ……… - ……… odbyło się szkolenie z zakresu egzaminu CompTIA Security+ (SY0-501).

Plan szkolenia:

1. Dnia …:
   1. …
   2. …
   3. etc.
2. Dnia …:
   1. …
   2. …
   3. etc.
3. etc.

W szkoleniu udział wzięli:

1. Dnia …:
   1. …
   2. …
   3. etc.
2. Dnia …:
   1. …
   2. …
   3. etc.
3. etc.

………………………………………………………………… ………………………………………………………

podpis osoby przeprowadzającej szkolenie podpis osoby odbierającej szkolenie

Załącznik nr 3 do umowy nr … z dnia …………

**Protokół odbioru egzaminu**

Warszawa, dnia …………

Protokół z przeprowadzonego egzaminu CompTIA Security+ SY0-501

W dniach ……… - ……… odbył się egzamin CompTIA Security+ SY0-501.

W egzamine udział wzięli:

1. …
2. …
3. …
4. …

………………………………………………………………… ………………………………………………………

podpis osoby przeprowadzającej egzamin podpis osoby odbierającej egzamin