

Stawiszyn 13.05.2026 r.

Załącznik nr 7 do SWZ

PFiZP 271.1.AGA.2026

OPIS PRZEDMIOTU ZAMÓWIENIA

Gmina i Miasto Stawiszyn

ul. Szosa Pleszewska 3,

62-820 Stawiszyn

1. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa przeprowadzenia szkoleń specjalistycznych oraz działań związanych z podnoszeniem świadomości cyberbezpieczeństwa.

2. Miejsce realizacji przedmiotu zamówienia

Miejsce realizacji przedmiotu zamówienia jest Urząd Gminy i Miasta Stawiszyn, ul. Szosa Pleszewska 3, 62-820 Stawiszyn.

3. Termin realizacji

Ostateczny termin wykonania przedmiotu zamówienia: 10.06.2026 r. Zamawiający przewiduje przedłużenie terminu realizacji w przypadku uzyskania zgody na przedłużenie realizacji projektu

4. Równoważność

Przedmiot zamówienia dotyczy szkoleń specjalistycznych realizowanych w środowisku opartym na konkretnych rozwiązaniach technologicznych (ESET / Fortinet / Holm Security / Microsoft Windows Server / Active Directory).

Ze względu na konieczność zapewnienia zgodności merytorycznej szkolenia z rzeczywistym środowiskiem Zamawiającego, szkolenia muszą być prowadzone wyłącznie w oparciu o wskazane rozwiązania producentów.

Wprowadzenie rozwiązań równoważnych uniemożliwiłoby osiągnięcie celów szkoleniowych, ponieważ różnice funkcjonalne pomiędzy systemami nie pozwalają na transfer wiedzy wymagany przez Zamawiającego.

Celem zamówienia jest podniesienie kompetencji w zakresie obsługi i administracji konkretnych systemów funkcjonujących lub planowanych do wdrożenia w infrastrukturze Zamawiającego.

Zamawiający podzielił zamówienie na 8 zadań:

- 1) Zadanie nr 1 - Przeprowadzenie szkolenia specjalistycznego ESET Protect Administrator
- 2) Zadanie nr 2- Przeprowadzenie szkolenia specjalistycznego ESET XDR Administrator
- 3) Zadanie nr 3 - Przeprowadzenie szkolenia specjalistycznego FortiGate Administrator
- 4) Zadanie nr 4 – Przeprowadzenie szkolenia specjalistycznego Obsługa Holm Security
- 5) Zadanie nr 5 – Kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness)
- 6) Zadanie nr 6 – Przeprowadzenie szkoleń stacjonarnych z zakresu świadomości cyberbezpieczeństwa
- 7) Zadanie nr 7 – Przeprowadzenie testów socjotechnicznych

8) Zadanie nr 8 - Przeprowadzenie szkolenia specjalistycznego Zarządzanie usługą Active Directory w środowisku Microsoft Windows Server

Zadanie nr 1

**Przeprowadzenie szkolenia specjalistycznego
ESET Protect Administrator**

Nazwa szkolenia	Liczba uczestników szkolenia
ESET Protect Administrator	1

Forma szkolenia	Szkolenie stacjonarne
czas trwania szkolenia	4 godziny
Język szkolenia	Polski <i>Jeżeli trener nie posługuje się językiem polskim Wykonawca zobowiązany jest zapewnić tłumaczenie</i>
Okres realizacji	Dostarczenie vouchera na szkolenie ważnego przez 12 miesięcy nastąpi do 7 dni od podpisania umowy
Przesłanki dla szkolenia	Z uwagi na fakt, iż Zamawiający użytkuje rozwiązania ESET konieczne jest podniesienie kompetencji personelu informatycznego w zakresie administracji tymi rozwiązaniami.
Program szkolenia / podstawowe kwestie poruszone na szkoleniu	Program szkolenia: - Szczegółowe omówienie elementów konsoli Eset Protect, - konfiguracji polityk bezpieczeństwa, - omówienie zarządzania komputerami, - konfiguracja sandbox, - konfiguracja MDM, - konfiguracja Full Disk Encryption
Egzamin	Niewymagany
Wymagania wobec wykładowcy / trenera	- Minimum 2-letnie doświadczenie z zakresu realizacji szkoleń dotyczących ESET Wymóg 2-letniego doświadczenia należy rozumieć jako przeprowadzenie co najmniej 2 szkoleń z tematyki objętej zakresem przedmiotu zamówienia w ciągu ostatnich 3 lat licząc wstecz od dnia opublikowania niniejszego zapytania. Przy

	<p>czym szkolenia były realizowane w ciągu 2 różnych lat kalendarzowych.</p> <p>Do oferty należy dołączyć referencje lub inne dokumenty potwierdzające wykonanie szkoleń</p> <p>- Dla zapewnienia wysokiego poziomu usług zamówienie musi być realizowane przez wykonawcę posiadającego aktywne certyfikaty producenta (firmę ESET)</p> <p>a) Certified ESET Managed Client Security Professional</p> <p>- Kopię certyfikatu należy dołączyć do oferty.</p>
Dodatkowe wymagania	<p>- Zamawiający planuje wdrożyć/wdrożył wyżej wymienione rozwiązania zgodnie z zaleceniami DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2). Do tego niezbędne mogą być konsultacje dotyczące zgodności z wyżej wymienioną dyrektywą lub Systemem Zarządzania Bezpieczeństwem Informacji Zamawiającego, wobec czego zaleca się, by wykonawca posiadał również co najmniej jeden certyfikat Audytora Wiodącego Systemu Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO/IEC 27001:2023-08.</p> <p>- Dokumenty potwierdzające spełnienie wymagań należy dołączyć do oferty.</p> <p>- Zamawiający wymaga dostarczenia imiennego zaświadczenia ukończenia szkolenia</p>

Zadanie nr 2

Przeprowadzenie szkolenia specjalistycznego ESET XDR Administrator

Nazwa szkolenia	Liczba uczestników szkolenia
ESET XDR Administrator	1

Forma szkolenia	Szkolenie stacjonarne
czas trwania szkolenia	8 godzin

Język szkolenia	Polski <i>Jeżeli trener nie posługuje się językiem polskim Wykonawca zobowiązany jest zapewnić tłumaczenie</i>
Okres realizacji	Dostarczenie vouchera na szkolenie ważnego przez 12 miesięcy nastąpi do 7 dni od podpisania umowy
Przesłanki dla szkolenia	Z uwagi na fakt, iż Zamawiający użytkuje rozwiązania ESET konieczne jest podniesienie kompetencji personelu informatycznego w zakresie administracji tymi rozwiązaniami.
Program szkolenia / podstawowe kwestie poruszone na szkoleniu	Program szkolenia: <ol style="list-style-type: none"> 1. Omówienie podstawowych pojęć związanych z Threat Huntingiem. 2. Przygotowanie playbook'a. 3. Wdrożenie serwera ESET Inspect on-prem – ćwiczenie. 4. Wdrożenie i konfiguracja ESET Inspect Connector – ćwiczenie. 5. Omówienie konsoli ESET Inspect oraz jakie dane zbiera XDR. 6. Podstawowe detekcje i reagowanie. 7. Uruchomienie podstawowej detekcji – ćwiczenie. 8. Weryfikacja incydentu. 9. Wykluczenia i ich tworzenie – ćwiczenie. 10. Przeprowadzenie analizy powłamaniowej – ćwiczenie. 11. Raportowanie i powiadomienia – ćwiczenie.
Egzamin	Niewymagany
Wymagania wobec wykładowcy / trenera	- Minimum 2-letnie doświadczenie z zakresu realizacji szkoleń dotyczących ESET Wymóg 2-letniego doświadczenia należy rozumieć jako przeprowadzenie co najmniej 2 szkoleń z tematyki objętej zakresem przedmiotu zamówienia w ciągu ostatnich 3 lat licząc wstecz od dnia opublikowania niniejszego zapytania. Przy czym szkolenia były realizowane w ciągu 2 różnych lat kalendarzowych. Do oferty należy dołączyć referencje lub inne dokumenty potwierdzające wykonanie szkoleń - Dla zapewnienia wysokiego poziomu usług zamówienie musi być realizowane przez wykonawcę

	posiadającego aktywne certyfikaty producenta (firmę ESET) - Kopię certyfikatu należy dołączyć do oferty.
Dodatkowe wymagania	- Zamawiający wymaga dostarczenia imiennego zaświadczenia ukończenia szkolenia

Zadanie nr 3

Przeprowadzenie szkolenia specjalistycznego FortiGate Administrator

Nazwa szkolenia	Liczba uczestników szkolenia
FortiGate Administrator	1

Forma szkolenia	Szkolenie stacjonarne
czas trwania szkolenia	12 godzin w podziale na sesje
Język szkolenia	Polski <i>Jeżeli trener nie posługuje się językiem polskim Wykonawca zobowiązany jest zapewnić tłumaczenie</i>
Okres realizacji	Dostarczenie vouchera na szkolenie ważnego przez 12 miesięcy nastąpi do 7 dni od podpisania umowy
Przesłanki dla szkolenia	Z uwagi na fakt, iż Zamawiający użytkuje rozwiązania Fortinet konieczne jest podniesienie kompetencji personelu informatycznego w zakresie administracji tymi rozwiązaniami.
Program szkolenia / podstawowe kwestie poruszone na szkoleniu	Program szkolenia: - Omówienie konta support.fortinet.com - Rejestracja urządzeń. - Omówienie wersjonowania FortiOS - Zarządzanie uprawnieniami dostępu - Wstępna konfiguracja. - Konfiguracja Portów (agregacja, redundancja), tworzenie VLAN'ów - Konfiguracja polityk bezpieczeństwa oraz profili bezpieczeństwa - Konfiguracja Antywirusa, IPS/IDS, Webfiltering'u, Antyspamu - Konfiguracja przekierowania portów (Virtual IP, port forwarding)

	<ul style="list-style-type: none"> - Logowanie danych - Obsługa kilku łączy WAN (failover, load balancing) - VPN – omówienie i konfiguracja połączeń klienckich, oraz Site to Site - Integracja z domeną i jej wykorzystanie - Uwierzytelnianie dwuskładnikowe - Kontrola aplikacji - Analiza ruchu szyfrowanego - Konfiguracja powiadomień o zdarzeniach - Backup/przywracanie ustawień urządzenia, uruchamianie i zarządzanie awaryjne. - Optymalizacja konfiguracji i monitorowania obciążenia systemu – dobre praktyki. - VDOM - praktyczne wykorzystanie - tryby transparent/nat. - SD-WAN - Load Balancing i failover łączy Internetowych, oraz połączeń VPN. - Routing dynamiczny na przykładzie połączeń VPN Site to Site. - Integracja z AD – FSSO (reguły firewall dla grup i użytkowników). - Głęboka Inspekcja SSL - jak skutecznie wdrożyć. - Tworzenie i obsługa sieci dla gości. - Dwuskładnikowa autoryzacja. - Debugowanie ruchu sieciowego oraz połączeń VPN za pomocą terminala. - Sposoby na awaryjne uruchamianie urządzenia po błędnej aktualizacji lub utracie hasła
Egzamin	Niewymagany
Wymagania wobec wykładowcy / trenera	<ul style="list-style-type: none"> - Minimum 2-letnie doświadczenie z zakresu realizacji szkoleń dotyczących cyberbezpieczeństwa oraz rozwiązań UTM <p>Wymóg 2-letniego doświadczenia należy rozumieć jako przeprowadzenie co najmniej 2 szkoleń z tematyki objętej zakresem przedmiotu zamówienia w ciągu ostatnich 3 lat licząc wstecz od dnia opublikowania niniejszego zapytania. Przy czym szkolenia były realizowane w ciągu 2 różnych lat kalendarzowych.</p> <p>Do oferty należy dołączyć referencje lub inne dokumenty potwierdzające wykonanie szkoleń</p> <ul style="list-style-type: none"> - Aktualny certyfikat potwierdzający wiedzę z zakresu szkolenia wydany przez producenta sprzętu

	<p>lub niezależną instytucję certyfikującą. Zamawiający będzie akceptował certyfikaty wydane przez producenta danego rozwiązania i powszechnie uznane certyfikaty informatyczne z obszaru szkolenia.</p> <ul style="list-style-type: none"> - Dla zapewnienia wysokiego poziomu usług zamówienie musi być realizowane przez wykonawcę na poziomie min. zaawansowanym, posiadającego aktywne specjalizacje: <ul style="list-style-type: none"> a) Fortinet Certified Solution Specialist Network Security b) w zakresie Krawędzi Usługi Bezpiecznego Dostępu (SASE), - Kopię certyfikatu należy dołączyć do oferty.
Dodatkowe wymagania	<ul style="list-style-type: none"> - Zamawiający planuje wdrożyć wyżej wymienione rozwiązania zgodnie z zaleceniami DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2). Do tego niezbędne mogą być konsultacje dotyczące zgodności z wyżej wymienioną dyrektywą lub Systemem Zarządzania Bezpieczeństwem Informacji Zamawiającego, wobec czego zaleca się, by wykonawca posiadał również co najmniej jeden certyfikat Audytora Wiodącego Systemu Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO/IEC 27001:2023-08. - Dokumenty potwierdzające spełnienie wymagań należy dołączyć do oferty. - Zamawiający wymaga dostarczenia imiennego zaświadczenia ukończenia szkolenia

Zadanie nr 4

Przeprowadzenie szkolenia specjalistycznego Obsługa Holm Security

Nazwa szkolenia	Liczba uczestników szkolenia
Obsługa Holm Security	1
Forma szkolenia	Szkolenie online

czas trwania szkolenia	Min. 6 godzin
Język szkolenia	Polski <i>Jeżeli trener nie posługuje się językiem polskim Wykonawca zobowiązany jest zapewnić tłumaczenie</i>
Okres realizacji	Dostarczenie vouchera na szkolenie ważnego przez 12 miesięcy nastąpi do 7 dni od podpisania umowy
Przesłanki dla szkolenia	Z uwagi na fakt, iż Zamawiający użytkuje rozwiązania Holm Security konieczne jest podniesienie kompetencji personelu informatycznego w zakresie administracji tymi rozwiązaniami.
Program szkolenia / podstawowe kwestie poruszone na szkoleniu	<p>Program szkolenia:</p> <ol style="list-style-type: none"> 1. Proces zarządzania podatnościami <ul style="list-style-type: none"> ○ Rodzaje podatności ○ Podatności w hostach ○ Podatności w aplikacjach webowych (OWASP Top 10) ○ Środowiska OT 2. Architektura Holm 3. Ćwiczenie praktyczne <ul style="list-style-type: none"> ○ Logowanie się do konsoli ○ Wdrożenie scanner appliance'a 4. Skanowanie aplikacji webowych – omówienie 5. Ćwiczenie praktyczne <ul style="list-style-type: none"> ○ Skonfigurowanie assetu – web aplikacja ○ Skonfigurowanie profilu skanowania dla web aplikacji 6. Skanowanie web aplikacji <ul style="list-style-type: none"> ○ Skanowanie bezagentowe – omówienie ○ Skanowanie typu discovery 7. Ćwiczenie praktyczne

	<ul style="list-style-type: none"> o wykonanie skanu discovery <p>8. Skanowanie hosta – omówienie</p> <p>9. Ćwiczenie praktyczne</p> <ul style="list-style-type: none"> o wykonanie skanu hosta <p>10. Skanowanie uwierzytelnione i niewierzytelnione – omówienie</p> <p>11. Moduł phishingowy</p> <ul style="list-style-type: none"> o OSINT o Socjotechnika o Omówienie modułu phishingowego o Przygotowanie phishingu <ul style="list-style-type: none"> ▪ Implementacje szablonów o Przeprowadzenie oceny phishingowej <p>12. Ćwiczenie praktyczne - przygotowanie kampanii phishingowej</p> <p>13. Moduł raportowy</p> <ul style="list-style-type: none"> o Generowanie przykładowych raportów – omówienie o Ćwiczenie praktyczne – Raportowanie <p>14. Podsumowanie</p> <ul style="list-style-type: none"> o Ćwiczenie praktyczne – Analiza wyników skanowania o Pytania
Egzamin	Niewymagany
Wymagania wobec wykładowcy / trenera	<p>- Minimum 2-letnie doświadczenie z zakresu realizacji szkoleń dotyczących Holm Security</p> <p>Wymóg 2-letniego doświadczenia należy rozumieć jako przeprowadzenie co najmniej 2 szkoleń z tematyki objętej zakresem przedmiotu zamówienia w ciągu ostatnich 3 lat licząc wstecz od dnia opublikowania niniejszego zapytania. Przy czym szkolenia były realizowane w ciągu 2 różnych lat kalendarzowych.</p> <p>Do oferty należy dołączyć referencje lub inne dokumenty potwierdzające wykonanie szkoleń</p>

	<p>- Dla zapewnienia wysokiego poziomu usług zamówienie musi być realizowane przez wykonawcę posiadającego aktywne certyfikaty producenta (firmę Holm Security)</p> <p>- Kopię certyfikatu należy dołączyć do oferty.</p>
Dodatkowe wymagania	<p>- Zamawiający wymaga dostarczenia imiennego zaświadczenia ukończenia szkolenia</p> <p>- Zamawiający wymaga dostarczenia imiennego certyfikatu wystawionego przez autoryzowane centrum szkoleniowe (pod warunkiem pozytywnego ukończenia egzaminu przez pracownika odbywającego szkolenie po stronie Zamawiającego).</p>

Zadanie nr 5

Kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness). Przedmiotem oferty jest kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie. Dedykowana jest dla 30 użytkowników Zamawiającego i świadczona przez okres 6 miesięcy.

Usługa musi zawierać:

1. Platformę szkoleniową zawierającą minimum 45 szkoleń, dostępnych w języku polskim (oraz w jęz. angielskim, niemieckim, hiszpańskim, czeskim, słowackim, serbskim, chorwackim i włoskim), w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.

a) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:

- ✓ Podstawy bezpiecznego internetu
- ✓ Bezpieczeństwo poczty
- ✓ Załączniki w poczcie elektronicznej
- ✓ Phishing
- ✓ Spyware/malware
- ✓ Bezpieczeństwo danych osobowych RODO/GDRP
- ✓ Bezpieczne hasła
- ✓ Menedżery haseł
- ✓ Bezpieczeństwo urządzeń mobilnych
- ✓ Uwierzytelnianie wieloskładnikowe (MFA)
- ✓ Bezpieczna praca zdalna
- ✓ Bezpieczna praca w biurze
- ✓ Sieci społeczne
- ✓ Socjotechnika stosowana
- ✓ Zakupy w internecie

b) Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.

c) Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin.

2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:

a) z linkiem prowadzącym do strony internetowej,

b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,

c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,

d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

3. dedykowaną platformę dostarczającą raporty obejmujące minimum:

a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,

b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zawierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akcję oraz szczegółowe daty wykonania tych operacji.

W ramach świadczonej usługi usługodawca musi:

- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,

- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,

- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,

- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,

- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 5 zmian w okresie trwania usługi).

Wymagania dodatkowe:

Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych

użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.

Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Do oferty należy załączyć oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.

Zadanie nr 6

Przeprowadzenie szkoleń stacjonarnych z zakresu świadomości cyberbezpieczeństwa.

1. Przedmiotem zamówienia jest realizacja usługi obejmującej:
 - a) Przeprowadzenie szkoleń stacjonarnych z zakresu świadomości cyberbezpieczeństwa dla maksymalnie 26 pracowników Zamawiającego.
 - b) Dostarczenie materiałów szkoleniowych.
2. Szkolenia będą podzielone na dwie grupy
 - a) Kadra pracowników biurowych Urzędu – 2 grupy szkoleniowe po 13 osób.
3. Szkolenia będą realizowane w formie stacjonarnej w siedzibie Zamawiającego.
4. Zamawiający zapewni salę szkoleniową oraz podstawowe wyposażenie (projektor/ekran; nagłośnienie - jeśli wymagane; dostęp do zasilania).
5. Wykonawca zapewni prowadzących, organizację szkoleń po swojej stronie oraz materiały szkoleniowe.
6. Szkolenie dla jednej grupy szkoleniowej – minimum 4 godziny szkoleniowe (lekcyjne).
7. Wszystkie szkolenia muszą być prowadzone w języku polskim na podstawie zaakceptowanego przez Zamawiającego harmonogramu.
8. Zamawiający wymaga prowadzenia dokumentacji – listy obecności uczestników szkolenia.
9. Każdy z uczestników szkolenia otrzyma materiały szkoleniowe w formacie pdf.
10. Szkolenia muszą obejmować minimum następujące zagadnienia:
 - a) Czym jest świadomość bezpieczeństwa
 - b) Motywy osób atakujących
 - c) Ochrona informacji i prywatność w Internecie.
 - d) Socjotechnika – stany emocjonalne wykorzystywane przez przestępców.
 - e) Ransomware jako poważne zagrożenie dla JST.
 - f) Jak rozpoznać fałszywe bramki płatności
 - g) Co zrobić, kiedy Twoje dane wyciekły
 - h) Dezinformacja w internecie
 - i) Polityka haseł



- j) Bezpieczne hasła i uwierzytelnianie dwuskładnikowe.
 - k) Metody przechowywania haseł
 - l) Phishing oraz inne zagrożenia związane z pocztą elektroniczną.
 - m) Cyberhigiena, w tym bezpieczeństwo urządzeń mobilnych.
 - n) Bezpieczeństwo pracy zdalnej.
 - o) Jakie dane publikujemy w portalach społecznościowych i czym mogą one grozić
 - p) Co robić, gdy nasze konto zostało przejęte
 - q) Jak zadbać o bezpieczeństwo naszych portali
 - r) Metody płatności w Internecie - dobre i złe strony
 - s) Czym jest charge back?
 - t) Jak podnieść bezpieczeństwo urządzenia mobilnego
 - u) Jak ochronić dane, jeżeli straciliśmy smartphone
 - v) Jak bezpiecznie przysyłać wrażliwe dane
 - w) Zabezpieczenie danych na komputerze
 - x) Polityka "czystego biurka"
11. Wykonawca zapewni poufność informacji uzyskanych w związku z realizacją zamówienia.
12. Jeżeli w toku realizacji dojdzie do przetwarzania danych osobowych (np. służbowe adresy e-mail), strony zawrą umowę powierzenia przetwarzania danych osobowych, o ile będzie wymagana.
13. Zamawiający wymaga, aby Wykonawca posiadał i utrzymywał przez cały okres realizacji zamówienia **certyfikowany System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001**.
14. Na potwierdzenie spełnienia wymagania Zamawiający wymaga przedstawienia **ważnego certyfikatu ISO/IEC 27001** wydanego przez **akredytowaną jednostkę certyfikującą** (lub certyfikatu równoważnego).

Zadanie nr 7

Przeprowadzenie testów socjotechnicznych w Urzędzie Miasta i Gminy w Stawiszynie.

1) Zakres testów będzie dotyczyć:

Testy zdalne:

a. Phishing (max. 2-3 scenariusze testowe):

- pozyskiwanie e-maili w publicznych źródłach,
- Zamawiający przewiduje możliwość udostępnienia adresów email pracowników, w przypadku, gdy podjęte przez Wykonawcę działania OSINT będą nie efektywne
- rejestracja odpowiednio podobnej domeny do domeny bazowej (wykorzystana będzie do dalszych kroków),
- wykonanie mailingów nakłaniających do podania hasła dostępowego do jednego z systemów,

- zastosowanie złośliwych linków i załączników zawierających oprogramowanie, które będzie służyło tylko do zbierania danych i odnotowania sukcesu ataku oraz było bezpieczne i nieszkodliwe dla organizacji, bez ryzyka paraliżu w zakresie świadczenia usług przez Zamawiającego, w szczególności bez ryzyka zaszyfrowania danych. Wykonawca zapewni, że „złośliwe” załączniki zawierać będą jedynie prosty program odsyłający na serwer Wykonawcy dane telemetryczne na temat zaatakowanej maszyny bez przejścia nad nią „całkowitej” kontroli,
- b. Vishing (1 scenariusz):
- pozyskiwanie telefonów w publicznych źródłach,
 - wykonanie telefonów nakłaniających do zainstalowania złośliwego oprogramowania (np. podanie się za technika sprawdzającego zgłoszony „problem” z dostępem do Internetu),
 - próba nakłonienia do nawiązania połączenia zdalnego z komputerem,
 - Zamawiający wymaga, aby raport z testów Vishing zawierał opis przyjętych założeń (w tym co do liczby scenariuszy i atakowanych pracowników), opis realizowanych scenariuszy oraz statystyki zgodne z zakresem kampanii (np. liczba osób, które przekazały poufne informacje, liczba przekazanych poświadczeń).

Testy stacjonarne on-site – (max. 3 scenariusze):

- c. próba fizycznego, nieautoryzowanego wejścia do pomieszczeń biurowych oraz uzyskania dostępu do budynku w godzinach wskazanych przez Zamawiającego,
- d. próba nakłaniania osób wewnątrz budynku do przekazania dostępu do komputera,
- e. próba nakłonienia pracownika do uruchomienia oprogramowania z dostarczonego pendrive,
- f. próby uzyskania dostępu do sieci wewnętrznej Zamawiającego, w sposób nie wpływający na przerwanie pracy czy długotrwałe uniemożliwienie świadczenia usług,
- g. Baiting, poprzez umieszczenie w siedzibie organizacji nośników danych zawierających oprogramowanie informujące o ich podłączeniu.

2) Lokalizacja

- a. budynek Urzędu Miasta i Gminy w Stawiszynie, ul. Szosa Pleszewska 3, 62-820 Stawiszyn

3) Raport

- a. Zamawiający wymaga sporządzenia raportu końcowego zawierającego realizację wszystkich przeprowadzonych scenariuszy, w tym reakcje pracowników, napotkane przeszkody, wykryte podatności, wykryte luki w zabezpieczeniach oraz rekomendacje i proponowane działania naprawcze.

- b. Raporty z realizacji usługi powinny zostać przygotowane w wersji elektronicznej, zgodnie z wymogami Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021-2027
- c. Zamawiający wymaga, aby raporty były oznaczone logotypami (zgodnie z zasadami określonymi w konkursie „Cyberbezpieczny Samorząd”),
- d. Zamawiający wymaga, aby cały zakres usługi wykonywanej przez Zamawiającego został wykonany z należytym profesjonalizmem i zachowaniem zasad etyki,
- e. Zamawiający wymaga, aby całość dokumentacji została wykonana w języku polskim.

II. TERMIN WYKONANIA ZAMÓWIENIA

Termin wykonania przedmiotu zamówienia:

Wykonawca zobowiązany jest zrealizować usługę w terminie do dnia 10.06.2026 r. z możliwością przedłużenia terminu, jeśli grantodawca wyrazi na to zgodę.

Zadanie nr 8

Przeprowadzenie szkolenia specjalistycznego

Zarządzanie usługą Active Directory w środowisku Microsoft Windows Server

Nazwa szkolenia	Liczba uczestników szkolenia
Zarządzanie usługą Active Directory	1

Forma szkolenia	Szkolenie online
czas trwania szkolenia	Min. 12 godzin w rozbiciu na dwa dni robocze
Język szkolenia	Polski <i>Jeżeli trener nie posługuje się językiem polskim Wykonawca zobowiązany jest zapewnić tłumaczenie</i>
Okres realizacji	Dostarczenie vouchera na szkolenie ważnego przez 12 miesięcy nastąpi do 7 dni od podpisania umowy
Przesłanki dla szkolenia	Z uwagi na fakt, iż Zamawiający użytkuje rozwiązania Microsoft Windows Server konieczne jest podniesienie kompetencji personelu informatycznego w zakresie administracji tymi rozwiązaniami.
Program szkolenia / podstawowe kwestie poruszone na szkoleniu	Program szkolenia: Moduł 1: Instalacja i konfiguracja kontrolerów domeny

	<ul style="list-style-type: none"> • Omówienie usług AD DS • Omówienie kontrolerów domeny usług AD DS • Wdrożenie kontrolera domeny • Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server 2022 <p>Moduł 2: Zarządzanie obiektami w AD DS</p> <ul style="list-style-type: none"> • Zarządzanie kontami użytkowników • Zarządzanie grupami w usługach AD DS • Zarządzanie obiektami typu komputer w AD DS • Wdrażanie i zarządzanie OU <p>Moduł 3: Zarządzanie zaawansowaną infrastrukturą AD DS</p> <ul style="list-style-type: none"> • Wprowadzenie do zaawansowanych wdrożeń AD DS • Wdrożenie rozproszonego środowiska AD DS • Konfiguracja relacji zaufania AD DS. <p>Moduł 4: Wdrażanie i zarządzanie lokacjami i repliką AD DS</p> <ul style="list-style-type: none"> • Omówienie replikacji usług AD DS • Konfigurowanie lokacji usług AD DS • Konfigurowanie i monitorowanie replikacji usług AD DS. <p>Moduł 5: Wdrażanie zasad grupy</p> <ul style="list-style-type: none"> • Wprowadzenie do zasad grupy • Wdrażanie i zarządzanie obiektami GPO (Group Policy Object) • Konfiguracja zakresu i przetwarzania obiektów GPO • Rozwiązywanie problemów z GPO <p>Moduł 6: Zarządzanie ustawieniami użytkowników za pomocą zasad grupy</p> <ul style="list-style-type: none"> • Wdrażanie szablonów administracyjnych • Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów • Konfiguracja preferencji zasad grupowych
Egzamin	Niewymagany
Wymagania wobec wykładowcy / trenera	<p>- Minimum 2-letnie doświadczenie z zakresu realizacji szkoleń dotyczących Microsoft</p> <p>Wymóg 2-letniego doświadczenia należy rozumieć jako przeprowadzenie co najmniej 2 szkoleń z tematyki objętej zakresem przedmiotu zamówienia w ciągu ostatnich 3 lat licząc wstecz od</p>



	<p>dnia opublikowania niniejszego zapytania. Przy czym szkolenia były realizowane w ciągu 2 różnych lat kalendarzowych.</p> <p>Do oferty należy dołączyć referencje lub inne dokumenty potwierdzające wykonanie szkoleń</p>
Dodatkowe wymagania	<ul style="list-style-type: none">- Zamawiający wymaga dostarczenia imiennego zaświadczenia ukończenia szkolenia- Zamawiający wymaga dostarczenia imiennego certyfikatu wystawionego przez autoryzowane centrum szkoleniowe (pod warunkiem pozytywnego ukończenia egzaminu przez pracownika odbywającego szkolenie po stronie Zamawiającego).