Fundusze Europejskie
na Rozwój Cyfrowy

Załącznik nr 1 do umowy

(1.1) PRZEPROWADZENIE SZKOLEŃ DLA PRACOWNIKÓW – BUDUJĄCE ŚWIADOMOŚĆ CYBERZAGROŻEŃ I SPOSOBÓW OCHRONY INFORMACJI (175 osób) w 2025r. i 2026r.

Opis przedmiotu zamówienia (OPZ)

Zamawiający oczekuje realizacji szkoleń: dwóch w 2025 roku i jednego w roku 2026 w okresie wdrożenia i trwania projektu „Cyberbezpieczny Samorząd" (2025 r. i 2026r.).

Szkolenia dla **175 pracowników Urzędu** budujące świadomość zagrożeń i sposobów ochrony informacji zgodnie z najnowszymi zaleceniami CSIRT NASK, ENISA (liczba osób do przeszkolenia może ulec zmianie o +/- 10% osób). Szkolenia realizowane przez trenerów w siedzibie Zamawiającego ul. Kościuszki 1 97-400 Bełchatów w godzinach pracy Urzędu (poniedziałek, środa-czwartek 7:30-15:30, wtorek 8:00-18:00) **w formie zajęć stacjonarnych.**
Grupa docelowa: pracownicy Urzędu.

Wykonawca zobowiązuje się do przeprowadzenia szkoleń zgodnie z wytycznymi w zakresie realizacji zasad równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz zasady równości kobiet i mężczyzn w ramach Funduszy Unijnych na lata 2021-2027 zamieszczonymi na stronie www.funduszeeuropejskie.gov.pl w szczególności wytycznych dotyczących zasad równościowych w ramach Funduszy Unijnych na lata 2021-2027.

Szkolenia muszą być dedykowane dla pracowników Urzędu i muszą być przeprowadzone przez doświadczonych trenerów posiadających stosowną wiedzę.

Wykonawca, w terminie **7 dni** od zawarcia umowy, jest zobowiązany do sporządzenia i uzgodnienia z Zamawiającym szczegółowego Harmonogramu realizacji szkoleń.
Zamawiający zastrzega sobie prawo wniesienia uwag do przedłożonego Harmonogramu.

Zamawiający wymaga realizacji szkoleń, zgodnie z zaakceptowanym przez Zamawiającego, szczegółowym zakresem merytorycznym szkolenia, opracowanym na podstawie **ramowego programu szkolenia** wskazanego przez Zamawiającego w niniejszym opisie przedmiotu zamówienia (Etap 1 – Etap 3).

Zamawiający wymaga opracowania i przekazania uczestnikom szkoleń materiałów szkoleniowych, obejmujących szczegółowy zakres szkolenia w formie papierowej i elektronicznej, zawierających szczegółowe informacje, które będą omawiane podczas szkolenia. Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia.
Wykonawca zobowiązany jest przeprowadzić **test wstępny** przed każdym zaplanowanym szkoleniem oraz **test końcowy** po zakończonym szkoleniu celem zbadania wzrostu poziomu kompetencji pracowników po przebytym szkoleniu. **W terminie 21 dni** po przeprowadzonym szkoleniu Wykonawca zobowiązany jest opracować i przedłożyć Zamawiającemu **analizę**

indywidualną ankiet pod kątem osiągnięcia celu, jakim jest wzrost kompetencji. Do przedmiotowej analizy Wykonawca przedłoży w pliku excel dane źródłowe będące podstawą przeprowadzonej analizy.

Po każdym zakończonym szkoleniu Wykonawca wystawi uczestnikom szkolenia imienne certyfikaty w wersji papierowej.

W ramach wynagrodzenia Wykonawca dostarczy Zamawiającemu materiały ze szkolenia, które to będzie mógł wykorzystać do przeszkolenia osób nieobecnych lub nowoprzyjętych.

Wszystkie opracowane materiały szkoleniowe, certyfikaty, harmonogramy, programy muszą zawierać informacje o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd" oraz logotypy **według wzoru przekazanego przez Zamawiającego**.
Zamawiający zastrzega, że ramowy zakres tematyki szkolenia może zostać zmodyfikowany przez Zamawiającego na każdym etapie realizacji zadania; w zależności od aktualnych potrzeb, zachodzących zmian i specyfiki Urzędu, w szczególności wdrożonego SZBI oraz musi odnosić się do aktualnych aktów prawnych, zagrożeń cyberbezpieczeństwa, narzędzi, metod ataków i obrony przed nimi.

Zamawiający zapewni: salę szkoleniową, dostęp do sieci Internet, rzutnik, nagłośnienie. Wykonawca zapewni: sprzęt niezbędny do praktycznych warsztatów/ćwiczeń w grupach - Zamawiający dopuszcza, żeby warsztaty odbywały się w grupach po 3 osoby (ćwiczenia praktyczne/studia przypadków), prezentacje multimedialne, dyskusje, quizy i testy wiedzy.

Wykonawca ponosi koszty ewentualnego dojazdu, noclegu, wyżywienia kadry wskazanej do realizacji przedmiotu zamówienia.

Zamawiający nie dopuszcza metod zdalnych. Szkolenie w grupach nie większych niż **50 osób** (dla jednej grupy).

1. Termin realizacji szkoleń:
   1) **Pierwsze szkolenie (jednodniowe) w 2025 r. w terminie do 3 miesięcy od dnia zawarcia umowy – 175 osób - grupy nie większe niż 50 osób** (szkolenie rozłożone w ciągu 7-21 dni) **x 8 godzin zajęć/dzień** (jedna grupa). Jednostką czasową szkolenia jest 1 godzina dydaktyczna (45 minut), w tym przewiduje się cztery przerwy trwające po 10 minut w ciągu dnia.
   2) **Drugie szkolenie (jednodniowe) w 2025 r. w terminie do 7 miesięcy od dnia zawarcia umowy – 175 osób - grupy nie większe niż 50 osób** (szkolenie rozłożone w ciągu 7-21 dni) **x 8 godzin zajęć/dzień** (jedna grupa). Jednostką czasową szkolenia jest 1 godzina dydaktyczna (45 minut), w tym przewiduje się cztery przerwy trwające po 10 minut w ciągu dnia.
   3) **Trzecie szkolenie (jednodniowe) do 28 lutego 2026 r. - 175 osób - grupy nie większe niż 50 osób** (szkolenie rozłożone w ciągu 7-21 dni) **x 8 godzin zajęć/dzień**

(jedna grupa). Jednostką czasową szkolenia jest 1 godzina dydaktyczna (45 minut), w tym przewiduje się cztery przerwy trwające po 10 minut w ciągu dnia.

RAMOWY ZAKRES I TEMATYKA SZKOLEŃ

I. Etap 1: szkolenie w 2025 r. w terminie do 3 miesięcy od dnia zawarcia umowy

1. TEMAT SZKOLENIA - OCHRONA DANYCH OSOBOWYCH I BEZPIECZEŃSTWO INFORMACJI

1) **Przepisy / akty prawne:** podstawowe akty prawne (RODO, UODO, KRI, KSC, NIS2) - kogo obowiązują; ochrona danych a dostęp do informacji publicznej; zgodność z prawem, warunki wyrażenia zgody, zgoda wyrażona przez dzieci; obowiązki informacyjne; prawa osób „żądania" osób których dane dotyczą; ocena skutków dla ochrony danych, zasada ograniczonego przechowywania i retencja danych
2) **Odpowiedzialność za naruszenie przepisów RODO:** odpowiedzialność ADO, odpowiedzialność pracowników,
3) **Wprowadzenie do SZBI: Znaczenie SZBI dla Urzędu.**
4) **Zachowania osób/ogólne zasady bezpieczeństwa:** przekazywanie informacji w rozmowie bezpośredniej i telefonicznej; poczta i emaile (e-maile z potwierdzonych źródeł – UDW, szyfrowanie załączników e-mail); wysyłka listów tradycyjnych; bezpieczeństwo dokumentów; wizerunek i nagrywanie głosu osoby (problematyka ochrony wizerunku w przypadku fotografowania lub filmowania wydarzeń publicznych w jednostce np. festiwale, apele, gale itp.- ochrona wizerunku na podstawie ustawy o prawach autorskich i prawach pokrewnych; polityka kluczy; korzystanie z komputerów służbowych; zapisywanie danych w folderach; hasła do komputerów i do programów użytkowych - indywidualizacja i zakaz udostępniania; archiwizacja dokumentów i czyszczenie dysków - kasowanie danych z poczty i dysku - kosz; przechowywanie danych.
5) **Rozpoznawanie i kwalifikacja incydentów cyberbezpieczeństwa:** definicja incydentu cyberbezpieczeństwa; typy incydentów i ich charakterystyka; przegląd narzędzi i technik identyfikacji incydentów.
6) **Protokoły postępowania przy incydentach:** przygotowanie planu reagowania na incydenty; etapy postępowania: od identyfikacji po eliminację skutków; przypadek praktyczny: symulacja reagowania na incydent.
7) **Komunikacja i raportowanie w kontekście incydentów:** wymagania dotyczące raportowania incydentów; efektywna komunikacja wewnętrzna i zewnętrzna podczas kryzysu; przykłady dokumentacji i raportów incydentów.
8) **Dyskusja - pytania i odpowiedzi:** Odpowiedzi na pytania uczestników szkolenia.

II. Etap 2: szkolenie w 2025 r. w terminie do 7 miesięcy od dnia zawarcia umowy

1. TEMAT SZKOLENIA - CYBERBEZPIECZEŃSTWO - NARZĘDZIA CYBERBEZPIECZEŃSTWA – JAK BEZPIECZNIE PRACOWAĆ, TOŻSAMOŚĆ ELEKTRONICZNA

1) **Wprowadzenie do Cyberbezpieczeństwa:** kluczowe pojęcia i zagrożenia w cyberprzestrzeni.
   a) **Phishing**: Rozpoznawanie i Reagowanie: definicja i rodzaje phishingu (spear phishing, whaling, vishing, smishing pharming spoofing spim scam); analiza przypadków: Jak rozpoznać podejrzane e-maile, wiadomości, połączenia.

b) **Warsztaty**: symulacja ataków, phishingowych: **praktyczne ćwiczenia w grupach**, analiza próbek phishingowych i próba identyfikacji zagrożeń; wykorzystanie narzędzi do symulacji i testowania reakcji.
c) **Ransomware**: mechanizmy i sposoby obrony: przegląd różnych typów ransomware; analiza przypadków: Jak ransomware infekuje systemy i jakie są jego skutki; sposoby zapobiegania atakom ransomware: kopie zapasowe, aktualizacje, sandboxing.
d) **Inne zagrożenia w sieci:** niebezpieczne linki / wiadomości SMS / e-mail; dostęp zdalny a bankowość elektroniczna; sztuczna inteligencja; Deepfake.

2) **Objawy zainfekowania komputera.**
3) **Aktualność systemów: analiza przypadków:** Jak nieaktualizowane systemy wpływają na bezpieczeństwo.
4) **Wyszukiwarki internetowe:** pozyskiwanie informacji oraz danych osobowych przy użyciu specjalnych komend wyszukiwarki.
5) **Wykorzystanie danych**: wykorzystanie pozyskanych danych przez cyberprzestępców (szantaże, korzyści majątkowe).
6) **Szyfrowanie danych i bezpieczne przechowywanie:** podstawy szyfrowania danych; narzędzia do szyfrowania dysków, plików, załączników w poczcie elektronicznej; praktyczne ćwiczenia: Szyfrowanie plików na różnych systemach operacyjnych.
7) **Bezpieczne przeglądanie internetu i VPN:** przeglądarki internetowe a bezpieczeństwo; korzyści z używania sieci VPN.
8) **Tożsamość elektroniczna:** co to jest tożsamość elektroniczna; metody weryfikacji tożsamości; usługi zaufania; podpisy elektroniczne; podpisywanie, znakowanie, weryfikacja dokumentów.
9) **Zabezpieczanie Połączeń Wi-Fi:** podatności sieci Wi-Fi; zalecane praktyki zabezpieczeń sieciowych; konfiguracja zabezpieczeń na routerach i punktach dostępowych; jak unikać oszustw i nieautoryzowanego dostępu do danych.
10) **Dyskusja** - pytania i odpowiedzi: odpowiedzi na pytania uczestników szkolenia; dyskusja na temat najnowszych trendów i rozwiązań w cyberbezpieczeństwie.

III. <u>Etap 3: szkolenie w terminie do 28 lutego 2026 r.</u>

1. CYBERBEZPIECZEŃSTWO – BEZPIECZEŃSTWO W MEDIACH SPOŁECZNOŚCIOWYCH I OCHRONA PRYWATNOŚCI, STANDARDY OCHRONY MAŁOLETNICH

1) **Wprowadzenie do bezpieczeństwa w mediach społecznościowych:** wstęp do bezpieczeństwa cyfrowego i mediów społecznościowych.
2) **Podstawowe zasady bezpieczeństwa na platformach społecznościowych:** typowe zagrożenia i ryzyka związane z użytkowaniem mediów społecznościowych; ustawienia prywatności i bezpieczeństwa.
3) **Identyfikacja i ochrona przed cyberprzemocą i cyberstalkingiem:** definicja i rodzaje cyberprzemocy; narzędzia i strategie obronne; przykłady realnych przypadków i ich rozwiązania.
4) **Bezpieczne dzielenie się informacjami:** zasady bezpiecznego udostępniania treści i informacji osobistych; wpływ ustawień prywatności na widoczność postów;
5) **Praktyczne warsztaty:** ustawianie opcji prywatności na różnych platformach.

6) **Narzędzia do monitorowania i zarządzania kontem:** oprogramowanie i aplikacje do monitorowania aktywności online; zarządzanie wieloma kontami i zapobieganie atakom; **Praktyczne warsztaty:** skuteczne wykorzystanie narzędzi do zarządzania; kiedy i jak zgłaszać naruszenie prywatności; procedury postępowania w przypadku włamania na konto; symulacja postępowania po wykryciu naruszenia prywatności.
7) **Standardy ochrony w Internecie:** zagrożenia w sieci; sposoby walki z zagrożeniami; monitorowanie aktywności w Internecie; monitorowanie w celu ustalenia lokalizacji.
8) **Dyskusja - pytania i odpowiedzi:** Odpowiedzi na pytania uczestników szkolenia.

(1.2) PRZEPROWADZENIE SZKOLEŃ SPECJALISTYCZNYCH DLA INFORMATYKÓW W ZAKRESIE ZASTOSOWANYCH ŚRODKÓW BEZPIECZEŃSTWA (3 osoby) 2025r.,2026r.

Opis przedmiotu zamówienia (OPZ)

Zamawiający wymaga zorganizowania szkolenia **dla 3 informatyków** z zakresu Administrowania systemem Windows Server, Zarządzania usługą Active Directory w środowisku Microsoft Windows Server 2019/2022 oraz Wirtualizacji Hyper-V, magazynowania i przetwarzania danych w środowisku Microsoft Windows Server 2019/2022.

Wykonawca zobowiązuje się do przeprowadzenia szkoleń zgodnie z wytycznymi w zakresie realizacji zasad równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz zasady równości szans kobiet i mężczyzn w ramach Funduszy Unijnych na lata 2021-2027 zamieszczonych na stronie internetowej www.funduszeeuropejskie.gov.pl w szczególności wytycznych dotyczących realizacji zasad równościowych w ramach Funduszy Unijnych na lata 2021-2027.

Zamawiający wymaga, aby każde z trzech szkoleń zorganizowane zostało dla maksymalnie dwóch pracowników jednocześnie oraz zamykało się w ramach czasowych 2 dni robocze po minimum 6 godz. dydaktycznych (45 min.), w tym przerwy.

Zamawiający wymaga, aby przeszkolenie pracowników obejmowało również formę warsztatów, w trakcie których będą realizowane ćwiczenia opisujące codzienną pracę administratora w zakresie wdrożonego oprogramowania, rozwiązywanie problemów oraz procedurę aktualizacji i rozbudowy.

Szkolenia muszą odbywać się w formule zdalnej, w czasie rzeczywistym, z wykorzystaniem dedykowanej platformy szkoleniowej udostępnionej przez Wykonawcę.
Wykonawca zapewni odpowiednie środowisko szkoleniowe, obejmujące:

- platformę do wideokonferencji z możliwością udostępniania ekranu i interakcji uczestników,
- wirtualne środowisko laboratoryjne umożliwiające praktyczne ćwiczenia,
- materiały dydaktyczne w formie elektronicznej.

Jeżeli Wykonawca organizuje metodę szkolenia w formie otwartej, dopuszcza się przeprowadzenie szkolenia w takiej formie, w terminie wynikającym z realizacji umowy.

Wykonawca musi zagwarantować szkolenia spełniające minimum poniższy ramowy program.

Zamawiający zastrzega, że ramowy program może być modyfikowany przez Zamawiającego w zależności od aktualnych potrzeb, zachodzących zmian i specyfiki Urzędu oraz zakresu wdrożonego SZBI na każdym etapie realizacji zadania.

W ramach organizacji każdego ze szkoleń Wykonawca zapewni materiały szkoleniowe. Wszystkie opracowane materiały szkoleniowe, certyfikaty, programy muszą zawierać informacje o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny Samorząd" oraz logotypy **według wzoru przekazanego przez Zamawiającego**.

Po każdym zakończonym szkoleniu Wykonawca wystawi uczestnikom szkolenia imienne certyfikaty w wersji papierowej potwierdzające udział w szkoleniu.

Zamawiający przewiduje przeprowadzenie szkoleń w następujących terminach:

<u>Pierwsze szkolenie w 2025 r. w terminie do 3 miesięcy od dnia zawarcia umowy</u>

I. Ramowy program szkolenia Administrowanie systemem Windows Server:

1. Wprowadzenie do administracji systemu Windows Server
   1) Wprowadzenie do systemu Windows Server.
   2) Wprowadzenie do systemu Windows Server Core.
   3) Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server.
2. Usługi zarządzania tożsamością w systemie Windows Server
   1) Wprowadzenie do AD DS.
   2) Wdrażanie kontrolerów domeny Windows Server.
   3) Wprowadzenie do usługi Azure AD.
   4) Wdrażanie zasad grupy.
   5) Wprowadzenie do usług certyfikatów Active Directory.
3. Usługi infrastruktury sieciowej w systemie Windows Server
   1) Wdrażanie i zarządzanie protokołem DHCP.
   2) Wdrażanie i zarządzanie systemem DNS.
   3) Wdrażanie i zarządzanie systemem IPAM.
   4) Usługi dostępu zdalnego w systemie Windows Server.
4. Serwery plików i zarządzanie pamięcią masową w systemie Windows Server
   1) Woluminy i systemy plików w systemie Windows Server.
   2) Wdrażanie udostępniania w systemie Windows Server.
   3) Wdrażanie rozwiązania Storage Spaces (przestrzeni dyskowych) w systemie Windows Server.
   4) Wdrażanie deduplikacji danych.
   5) Wdrażanie interfejsu Iscsi.
   6) Wdrażanie rozproszonego systemu plików.
5. Wirtualizacja Hyper-V i kontenery w systemie Windows Server
   1) Hyper-V w systemie Windows Server.
   2) Konfiguracja maszyn wirtualnych.
   3) Zabezpieczanie wirtualizacji w systemie Windows Server.
   4) Kontenery w systemie Windows Server.
   5) Wprowadzenie do platformy Kubernetes.
6. Wysoka dostępność w systemie Windows Server
   1) Planowanie wdrożenia klastra pracy awaryjnej.
   2) Tworzenie i konfiguracja klastra pracy awaryjnej.
   3) Wprowadzenie do rozciągniętych klastrów.
   4) Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V.
7. Odzyskiwanie danych po awarii w systemie Windows Server
   1) Funkcja Hyper-V Replica.
   2) Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server.

8. Bezpieczeństwo systemu Windows Server
   1) Ochrona danych uwierzytelniających i dostępu uprzywilejowanego.
   2) Hardening systemu Windows Server.
   3) JEA w systemie Windows Server.
   4) Zabezpieczanie i analiza ruchu w SMB.
   5) Zarządzanie aktualizacjami w systemie Windows Server.
9. RDS (usługi pulpitu zdalnego) w systemie Windows Server
   1) Wprowadzenie do RDS.
   2) Konfiguracja wdrażania pulpitu opartego na sesji.
   3) Wprowadzenie do osobistych i połączonych pulpitów wirtualnych.
10. Dostęp zdalny i usługi internetowe w systemie Windows Server
    1) Wdrażanie sieci VPN.
    2) Wdrażanie usługi Always On VPN.
    3) Wdrażanie systemu NPS.
    4) Wdrażanie serwera WWW w systemie Windows Server.
11. Monitorowanie serwera i wydajności w systemie Windows Server
    1) Wprowadzenie do narzędzi do monitorowania systemu Windows Server.
    2) Korzystanie z monitora wydajności.
    3) Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów.
12. Aktualizacja i migracja w systemie Windows Server
    1) Migracja AD DS.
    2) Usługa migracji pamięci masowej.
    3) Narzędzia do migracji systemu Windows Server.

<u>Drugie szkolenie w 2025 r. w terminie do 7 miesięcy od dnia zawarcia umowy</u>

II. Ramowy program szkolenia Zarządzanie usługą Active Directory w środowisku Microsoft Windows Server 2019/2022:

1. Instalacja i konfiguracja kontrolerów domeny
   1) Omówienie usług AD DS.
   2) Omówienie kontrolerów domeny usług AD DS.
   3) Wdrożenie kontrolera domeny.
   4) Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server 2022.
2. Zarządzanie obiektami w AD DS.
   1) Zarządzanie kontami użytkowników.
   2) Zarządzanie grupami w usługach AD DS.
   3) Zarządzanie obiektami typu komputer w AD DS.
   4) Wdrażanie i zarządzanie OU.
3. Zarządzanie zaawansowaną infrastrukturą AD DS.
   1) Wprowadzenie do zaawansowanych wdrożeń AD DS.
   2) Wdrożenie rozproszonego środowiska AD DS.
   3) Konfiguracja relacji zaufania AD DS.
4. Wdrażanie i zarządzanie lokacjami i repliką AD DS.

1) Omówienie replikacji usług AD DS.
2) Konfigurowanie lokacji usług AD DS.
3) Konfigurowanie i monitorowanie replikacji usług AD DS.

5. Wdrażanie zasad grupy
1) Wprowadzenie do zasad grupy.
2) Wdrażanie i zarządzanie obiektami GPO (Group Policy Object).
3) Konfiguracja zakresu i przetwarzania obiektów GPO.
4) Rozwiązywanie problemów z GPO.

6. Zarządzanie ustawieniami użytkowników za pomocą zasad grupy
1) Wdrażanie szablonów administracyjnych.
2) Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów.
3) Konfiguracja preferencji zasad grupowych.

Trzecie szkolenie do 28 lutego 2026 roku

III. Ramowy program szkolenia: Wirtualizacja Hyper-V, magazynowanie i przetwarzanie danych w środowisku Microsoft Windows Server 2019/2022:

1. Omówienie funkcji administracyjnych systemu Windows Server
1) Informacje wstępne o systemie Windows Server 2019.
2) Omówienie najważniejszych funkcji systemu Windows Server.
3) Omówienie zasad i narzędzi związanych z zarządzaniem systemem Windows Server.

2. Zarządzanie serwerami plików i pamięcią masową w systemie Windows Server
1) Wolumeny i systemy plików w systemie Windows Server.
2) Współużytkowanie zasobów w systemie Windows Server.
3) Wdrażanie obszarów pamięci masowej w systemie Windows Server.
4) Wdrażanie funkcji deduplikacji danych.
5) Wdrażanie protokołu ISCSI.
6) Wdrażanie rozproszonego systemu plików.
7) Migracja magazynu danych w Windows Server 2022.

3. Oprogramowanie do wirtualizacji Hyper-V i kontenery w systemie Windows Server
1) Hyper-V w systemie Windows Server.
2) Konfigurowanie maszyn wirtualnych.
3) Zabezpieczenie wirtualizacji w systemie Windows Server.
4) Ulepszenia działania wirtualnego przełącznika sieciowego w Windows Server 2022.
5) Kontenery w systemie Windows Server.

4. Funkcje wysokiej dostępności w systemie Windows Server
1) Planowanie wdrażania klastrów na potrzeby przełączania awaryjnego.
2) Tworzenie i konfigurowanie klastra przełączania awaryjnego.
3) Omówienie klastrów rozległych.
4) Funkcje wysokiej dostępności i rozwiązania do usuwania skutków awarii oparte na maszynach wirtualnych Hyper-V.

5. Usuwanie skutków awarii w systemie Windows Server
1) Funkcja Hyper-V Replica.
2) Infrastruktura tworzenia i odtwarzania kopii zapasowych w systemie Windows Server.

6. Implementowanie i zarządzanie zasobami typu failover clustering
   1) Planowanie strategii wdrożenia typu failover cluster.
   2) Tworzenie i konfiguracja struktury failover cluster.
   3) Monitoring infrastruktury.
7. Implementowanie rozwiązań typu failover clustering dla maszyn wirtualnych w Hyper-V
   1) Prezentacja i integracja Hyper-V w Windows Server 2016 wraz z failover clustering.
   2) Implementacja i zarządzanie maszynami wirtualnymi w Hyper-V w failover clusters.
   3) Główne cechy wdrożeń maszyn wirtualnych w środowisku typu wysokiej dostępności i niezawodności.
   4) Szyfrowane Cluster Shared Volumes w Windows Server 2022.
8. Implementowanie network load balancing
   1) Przegląd metod zastosowania klastrów typu NLB.
   2) Konfiguracja klastrów NLB.
   3) Planowanie i implementacja NLB.

(1.3) USŁUGA DOSTĘPU DO PLATFORMY SZKOLENIOWEJ Z ZAKRESU ŚWIADOMOŚCI BEZPIECZEŃSTWA – DO POSZERZANIA ŚWIADOMOŚCI UŻYTKOWNIKÓW W ZAKRESIE CYBERBEZPIECZEŃSTWA, LICENCJA Z SUBSKRYPCJĄ dla 200 użytkowników do 30 kwietnia 2026r.

Przedmiotem oferty jest usługa szkolenia e-learningowego na kompleksowej platformie szkoleniowej on-line umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu cyberbezpieczeństwa - licencja z subskrypcją na 200 użytkowników.

Wykonawca w trakcie realizacji zamówienia zobligowany jest do zapewnienia dostępności dla osób ze szczególnymi potrzebami.

Wykonawca zobowiązuje się do przeprowadzenia szkoleń zgodnie z wytycznymi w zakresie realizacji zasad równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz zasady równości szans kobiet i mężczyzn w ramach Funduszy Unijnych na lata 2021-2027 zamieszczonych na stronie internetowej www.funduszeeuropejskie.gov.pl w szczególności wytycznych dotyczących realizacji zasad równościowych w ramach Funduszy Unijnych na lata 2021-2027.

Okres dostępu do platformy szkoleniowej: Platforma szkoleniowa musi być uruchomiona i dostępna dla wszystkich uczestników w sposób **ciągły w terminie 90 dni od zawarcia umowy do 30 kwietnia 2026 r.**

Zamawiający przewiduje łączną liczbę uczestników szkoleń w ilości 200 użytkowników z możliwością zmiany ilości o +/- 10% użytkowników.

Szkolenia muszą być dedykowane dla pracowników Urzędu i muszą być przeprowadzone przez doświadczonych trenerów posiadających stosowną wiedzę.

Zamawiający wymaga atrakcyjnej formy przekazu materiału szkolenia zachęcającej uczestników do aktywnego odbywania szkolenia. Atrakcyjna forma to m. in. grafika oparta na scenkach, postaciach, dialogach, przykładach, ćwiczeniach, testach sprawdzających wiedzę oraz dźwięk. Nie mogą to być same zdjęcia, definicje lub zagadnienia opisane w formie tekstowej i odtwarzane w postaci dźwiękowej.
Szkolenia muszą posiadać interaktywną formę, zwiększającą zaangażowanie osób biorących w nich udział. Szkolenie musi posiadać wysoką jakość merytoryczną przygotowanego scenariusza.

Szkolenia muszą wzbogacić wiedzę teoretyczną uczestników poprzez praktyczne ćwiczenia oraz zachęcić do aktywnego udziału. Muszą zostać wyposażone w elementy interakcji (np. kliknięcia, ćwiczenia), tak aby uczestnik był aktywny podczas szkolenia i nie miał możliwości zaliczenia szkolenia w sposób bierny tj. poprzez samoczynne odtworzenia filmu/ szkolenia.
Tematy szkolenia muszą kłaść duży nacisk na umiejętności praktyczne, nie tylko teorię bezpieczeństwa IT. W celu zwiększenia praktycznej przydatności szkolenia musi ono zostać opracowane tak, aby zajęcia kładły większy nacisk na umiejętności praktyczne użytkowników

komputerów (np. wykrywanie sytuacji zagrożenia, właściwe postępowanie w razie incydentu) niż samą teorię bezpieczeństwa IT.
Cały materiał szkolenia musi być dostępny w języku polskim i przedstawiony w sposób zrozumiały przez osoby nietechniczne.

Wymagania:

- **Środowisko pracy:**
  Platforma e-learningowa musi być dostępna z poziomu przeglądarek internetowych Firefox, Chrome, Edge dla systemów Windows 10 / 11 w aktualnych wersjach.
- **WCAG:**
  platforma musi spełniać wymagania standardu minimum WCAG 2.0 i musi być dostosowywana w okresie obowiązywania umowy do zachodzących zmian względem obowiązujących przepisów prawa.
- **Obligatoryjnie**:
  Jeżeli platforma nie spełnia wymagań standardów ustawy o dostępności cyfrowej, to musi posiadać moduł do wysyłania zgłoszeń pomocy technicznej przez osoby niepełnosprawne. Wykonawca w takim przypadku zobowiązany jest do udzielenia wszelkiej pomocy technicznej oraz merytorycznej uczestnikowi szkolenia.
- **Zasady działania pomocy technicznej**:
  Zgłoszenia pomocy technicznej i komunikacja z Wykonawcą odbywać się będą w języku polskim w godzinach pracy Urzędu, poprzez udostępniony przez Wykonawcę dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim. **Czas reakcji Wykonawcy nie może być dłuższy niż 3 godziny** w godzinach pracy Urzędu - **reakcja w postaci odpowiedzi na zgłoszenie w portalu serwisowym udostępnionym przez Wykonawcę. Brak dostępu do platformy szkoleniowej nie może być dłuższy niż 24 godziny od zgłoszenia (nie dotyczy dni wolnych od pracy Urzędu).**
- **SLA - gwarantowany poziom świadczenia usług:**
  Dostępność platformy – na poziomie minimum 97% przez cały okres realizacji zamówienia.
  Nielimitowany transfer danych.
  Codzienna kopia zapasowa danych.
  Platforma zabezpieczona certyfikatem SSL.
  Minimalna ilość łącznych dostępów uczestników do platformy w tym samym czasie na poziomie nie mniejszym niż 90%.

- **Wymagania dodatkowe:**
  Dostępność cyfrowa – platforma spełni wymagania ustawy o dostępności cyfrowej.
  Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej.
  Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.

- **Zobowiązania Wykonawcy:**

Po zakończeniu na platformie przez użytkowników wszystkich szkoleń Wykonawca wystawi każdemu uczestnikowi szkolenia jeden imienny certyfikat w wersji papierowej potwierdzający udział w poszczególnych szkoleniach. **Użytkownicy zakończą wszystkie szkolenia do dnia 20.02.2026 r.**

1. **Moduł platformy szkoleniowej:**

Platforma szkoleniowa zawierająca minimum **13 szkoleń,** dostępnych w języku polskim minimum w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego. **Wykonawca zobowiązany jest przeprowadzić test wstępny dla wszystkich użytkowników przed przystąpieniem do dedykowanych szkoleń oraz test końcowy po zakończonych szkoleniach celem zbadania wzrostu poziomu kompetencji pracowników po przebytych szkoleniach.**
W terminie 21 dni po odbyciu wszystkich szkoleń przez użytkowników Wykonawca zobowiązany jest opracować i przedłożyć Zamawiającemu **analizę indywidualną ankiet pod kątem osiągnięcia celu, jakim jest wzrost kompetencji.** Do przedmiotowej analizy Wykonawca przedłoży w pliku excel dane źródłowe będące podstawą przeprowadzonej analizy.

Szkolenia muszą zapewniać podniesienie kompetencji co najmniej w zakresie:

1) Czym jest bezpieczeństwo informacji i kto jest za nie odpowiedzialny/ Bezpieczeństwo informacji a ochrona danych osobowych i prywatności (minimum 1,5 godziny).
2) Zabezpieczenia stosowane w celu skutecznej ochrony informacji i danych osobowych/dobre praktyki (minimum 1,5 godziny).
3) Jak rozpoznawać i w jaki sposób reagować na incydenty bezpieczeństwa/Zagrożenia (minimum 1 godzina).
4) Bezpieczeństwo poczty/załączniki w poczcie elektronicznej (minimum 1,5 godziny).
5) Bezpieczna praca zdalna/Jak bezpiecznie pracować z urządzeniami mobilnymi (minimum 1 godzina).
6) Uwierzytelnianie wieloskładnikowe (MFA) (minimum pół godziny).
7) Zasady korzystania z bezpiecznych haseł/Jak bezpiecznie korzystać z menedżera haseł w praktyce **(minimum 1 godzina).**
8) Podstawy bezpiecznego Internetu/Jakie zagrożenia czyhają na użytkowników Internetu (minimum 1 godzina).
9) Bezpieczne korzystanie z urządzeń i aplikacji/ Zarządzanie uprawnieniami aplikacji (minimum 1 godzina).
10) Bezpieczeństwo w zakresie płatności elektronicznych (minimum 1 godzina).
11) Zasady korzystania z portali społecznościowych **(minimum pół godziny).**
12) Metody pozyskiwania informacji (Socjotechnika) (minimum pół godziny).
13) Techniki stosowane przez cyberprzestępców/Ransomware, malware, phishing (minimum 2 godziny).

(ww. zakresy szkoleń aktualizowane są na bieżąco przez Wykonawcę w konsultacji z Zamawiającym w odniesieniu do zachodzących zmian na rynku w dziedzinie cyberbezpieczeństwa i cyberzagrożeń), co zostanie uwzględnione w Harmonogramie szkoleń.

Łączny czas trwania wszystkich szkoleń powinien wynosić **co najmniej 14 godzin.**

2. **Moduł platformy phishingowej:**

Dedykowana platforma phishingowa pozwala na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników (tzw. kampania phishingową/atak

phishingowy). Platforma musi dostarczać scenariusze ataków z wykorzystaniem i naciskiem na aktualnie wykrywane i zidentyfikowane zagrożenia związane z atakami phishingowymi (w tym dostarczać ich wersję polskojęzyczną), posiadać bogaty zbiór predefiniowanych kampanii phishingowych związanych z wieloma różnymi branżami związanymi i niezwiązanymi bezpośrednio z działalnością Zamawiającego.

Platforma w ramach kampanii phishingowej musi generować **co najmniej poniższe typy wiadomości e-mail:**

1) z linkiem prowadzącym do strony internetowej,
2) 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,
3) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,
4) z załącznikiem o różnym rozszerzeniu co najmniej: .docx, .doc, .xlsx, .xls, .pdf, .zip,
5) zawierającym potencjalnie niebezpieczny kod.

Każdorazowe skuteczne przeprowadzenie akcji phishingowej musi kończyć się elementem edukacyjnym wyjaśniającym, gdzie użytkownik popełnił błąd. Platforma musi posiadać możliwość automatycznego skierowania użytkownika, który był podatny na oszustwo, na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

3. **Moduł raportowania:**

Dedykowana platforma generuje raporty obejmujące minimum:

1) status wykonania szkoleń przez poszczególnych użytkowników z uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,
2) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy był podatny na oszustwo, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akcję oraz szczegółowe daty wykonania tych operacji.

W ramach udostępnionej platformy Wykonawca musi:

1) zapewnić kompletność wszystkich usług wspomagających dla całego procesu wdrożeniowego, co oznacza brak potrzeby korzystania przez Zamawiającego z usług stron trzecich,
2) świadczyć serwis oraz wsparcie techniczne w całym okresie obowiązywania umowy,
3) dostarczyć materiał wideo z instrukcją obsługi platformy dla użytkowników końcowych zawierający co najmniej: Informację o tym do czego służy platforma, instrukcję pierwszego logowania do platformy, pierwsze kroki na platformie szkoleniowej.
4) przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości

phishingowych z platformy do użytkowników - wykaz imienny uczestników wraz z adresami e-mail zostanie przekazany Wykonawcy wyłonionemu w niniejszym postępowaniu na etapie podpisywania umowy.

5) zaproponować do akceptacji Zamawiającego szczegółowy Harmonogram szkoleń i kampanii phishingowych dopasowany do okresu świadczenia usługi,
6) zaplanować na podstawie Harmonogramu szkolenia i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
7) dostarczać pełny raport z realizacji szkoleń dla użytkowników po zakończeniu każdego zakresu tematycznego szkolenia oraz po przeprowadzonych kampaniach phishingowych oraz zbiorcze raporty końcowe,
8) wprowadzić zmiany w Harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji - zmian kolejności szkoleń lub liczby użytkowników, zmian dotyczących przeprowadzenia kampanii phishingowej.