Załącznik nr 3 do SWZ

Kancelaria Prezesa Rady Ministrów
Al. Ujazdowskie 1/3
00-583 Warszawa

FORMULARZ OFERTY

w postępowaniu pn. **„Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa w ramach 3 części:**

Część 1 - Szkolenie administratorów systemów informatycznych z Fortinet® realizowane na rzecz Rządowego Centrum Bezpieczeństwa;

Część 2 - Szkolenie administratorów systemów informatycznych z AI realizowane na rzecz Rządowego Centrum Bezpieczeństwa;

Część 3 - Szkolenie administratorów systemów informatycznych realizowane z systemów rodziny MS Windows na rzecz Rządowego Centrum Bezpieczeństwa", nr TP-31/26

Dane Wykonawcy/ Wykonawców wspólnie ubiegających się o udzielenie zamówienia:

Nazwa/firma Wykonawcy .....

Adres siedziby .....

NIP..... Regon.....

Nr KRS lub innego rejestru Wykonawcy (jeżeli dotyczy) .....

Nazwa rejestru i adres strony internetowej ogólnodostępnej bazy danych, z której Zamawiający może samodzielnie pobrać odpis z odpowiedniego rejestru Wykonawcy : .....

Osoba upoważniona do kontaktu:

Imię i nazwisko.....

telefon:.....

e-mail: .....

nazwa konta Wykonawcy na Platformie e-Zamówienia:.....

Wykonawca składający ofertę[1]:

□ jest mikroprzedsiębiorcą,

[1] proszę zaznaczyć właściwe

□ jest małym przedsiębiorcą,

□ jest średnim przedsiębiorcą,

□ prowadzi jednoosobową działalność gospodarczą,

□ jest osobą fizyczną nieprowadzącą działalności gospodarczej,

□ inny rodzaj.

1. W odpowiedzi na ogłoszenie o zamówieniu oświadczamy, że zrealizujemy ww. zamówienie, w zakresie określonym w opisie przedmiotu zamówienia, zgodnie z wymaganiami Zamawiającego wskazanymi w Specyfikacji Warunków Zamówienia, w tym w OPZ i PPU**, za cenę ogółem oferty ..... zł brutto**, w tym:
   a) Część 1 - Szkolenie administratorów systemów informatycznych z Fortinet® realizowane na rzecz Rządowego Centrum Bezpieczeństwa, za **..... zł brutto**;
   b) Część 2 - Szkolenie administratorów systemów informatycznych z AI realizowane na rzecz Rządowego Centrum Bezpieczeństwa, za **..... zł brutto**;
   c) Część 3 - Szkolenie administratorów systemów informatycznych realizowane z systemów rodziny MS Windows na rzecz Rządowego Centrum Bezpieczeństwa, za **..... zł brutto**.
2. Oświadczam, że przedmiot dostawy posiada następujące funkcjonalności/parametry :

   W celu prawidłowego wypełnienia poniższej tabeli należy w miejscach oznaczonych:
   – jedną gwiazdką (*) wybrać właściwą opcję a niewłaściwą skreślić lub wykasować

   W przypadku braku zaznaczenia/wypełnienia pola, Zamawiający uzna, że oferowane rozwiązanie nie spełnia danego parametru i tym samym uzna ofertę za podlegającą odrzuceniu.

Część 1: **Szkolenie administratorów systemów informatycznych z Fortinet® realizowane na rzecz Rządowego Centrum Bezpieczeństwa:**

L.p.	Wymagania minimalne które musi spełnić proponowane szkolenie	Proponowane szkolenie spełnia/nie spełnia wymagań
1	**1.1. Wymagany zakres szkolenia FortiGate:** Szkolenie powinno obejmować co najmniej następujące zagadnienia: - architektura urządzenia; - omówienie sposobu działania urządzenia FortiGate: ✓ jak urządzenie przetwarza ruch;	SPEŁNIA/ NIE SPEŁNIA*

	✓ polityki zapory sieciowej: • koncepcja firewall w urządzeniach FortiGate; • tworzenie obiektów dla reguł firewall; • translacja adresów NAT i Virtual IP; • internet Service Database; - inspekcja ruchu SSL i metody dystrybucji certyfikatów; - omówienie trybów pracy urządzenia – Proxy i Flow; - logowanie i powiadomienia; - wprowadzenie do Security Fabric, Fabric Connectors. - konfiguracja funkcji ochronnych (profile bezpieczeństwa): ✓ ochrona antywirusowa i integracja z FortiSandbox; ✓ system IPS / DoS Policy; ✓ kontrola ruchu WWW / blokowanie URL; ✓ DNS Filter; ✓ kontrola aplikacji; ✓ optymalizacja ruchu sieciowego (kształtowanie pasma). - VDOM - wirtualizacja w obrębie urządzenia; - wykorzystanie trybów pracy NAT / Transparent; - zaawansowana konfiguracja sieci i routingu, ✓ tworzenie sieci VLAN; ✓ SD-WAN - Load Balancing oraz redundancja łącz Internetowych; - uwierzytelnianie użytkowników: ✓ integracja z usługami katalogowymi – FSSO; ✓ tworzenie reguł firewall w oparciu o grupy użytkowników; ✓ konta użytkowników gości; ✓ dwuskładnikowa autoryzacja – FortiToken. - wirtualne sieci prywatne – VPN, IPSec VPN site-to-site, client-to-site; - konfiguracja urządzeń do pracy w klastrze HA, tryby pracy klastra, topologia połączeń i konfiguracja urządzeń; - możliwości diagnostyczne urządzenia, możliwości CLI, Sniffer jako podstawowe narzędzie, debug flow; - podejście do analizy problemów - jak być gotowym; - diagnostyka VPN, diagnostyka zapory, diagnostyka routingu. **1.2. Wymagany zakres szkolenia FortiAnalyzer:** Szkolenie powinno obejmować co najmniej następujące zagadnienia: ✓ wprowadzenie i wstępna konfiguracja FortiAnalyzer. ✓ możliwości FortiAnalyzer; ✓ rodzina produktów FortiAnalyzer; ✓ logowanie i raporty — zasada działania; ✓ ustawienia fabryczne, interfejs zarządzania; ✓ konfiguracja ustawień sieciowych; ✓ backup i odtwarzanie konfiguracji; ✓ komunikacja ze środowiskiem chmury publicznej. - administracja:	

	✓ konta i uprawnienia administracyjne; ✓ monitorowanie zdarzeń i zadań; ✓ domeny administracyjne; ✓ konfiguracja dysków RAID. - rejestracja urządzeń: ✓ lista urządzeń; ✓ dodawanie nowych urządzeń; ✓ Disk Quota; ✓ diagnostyka i rozwiązywanie problemów komunikacyjnych; ✓ zarządzanie zarejestrowanymi urządzeniami. - logi i archiwa: ✓ przetwarzanie i przeglądanie logów; ✓ przeszukiwanie logów; ✓ agregacja logów; ✓ przekazywanie logów; ✓ przywracanie logów; ✓ archiwizacja logów; ✓ alerty; ✓ archiwizacja, ✓ kwarantanna. - alarmowanie i system SOC: ✓ tworzenie alarmów; ✓ tworzenie event handlerów; ✓ zarządzanie incydentami bezpieczeństwa; ✓ wykorzystanie automatyzacji Playbooków. - raporty: ✓ tworzenie i generowanie raportów; ✓ zapytania SQL, ✓ wykresy; ✓ przeglądanie raportów; ✓ kalendarz raportów. - mechanizmy dodatkowe: ✓ konfiguracja systemu Indicator of Compromise; ✓ implementacja FortiGuard Outbreak Alert service; ✓ wykorzystanie asystenta AI. **1.3. Wymagany zakres szkolenia FortiMail:** Szkolenie powinno obejmować co najmniej następujące zagadnienia: - wstępna konfiguracja FortiMail w trybie Gateway: ✓ Zasada działania DNS; - konfiguracja chronionej domeny: ✓ pojedynczy serwer pocztowy; ✓ loadbalancing na wiele serwerów pocztowych. - obsługa SMTP przez FortiMail: ✓ fortimail jako MTA dla poczty przychodzącej i wychodzącej; ✓ weryfikacja adresów odbiorców;	

	✓ fortiMail jako proxy dla sesji uwierzytelnionych. - konfiguracja i omówienie reguł Access Control; - opracowanie niezbędnych polityk do poprawnej obsługi ruchu; - omówienie zasad działania reguł: ✓ ip policies; ✓ recipient policies. - analiza logów; - troubleshooting; - omówienie i konfiguracja profilu sesji; - profile antyspamowe dla ruchu przychodzącego; - antyspam dla ruchu wychodzącego; - relay host; - profile antywirusowe: ✓ omówienie oraz konfiguracja integracji z FortiSandbox. - profile kontroli treści; - DLP; - Block / Safe listy; - filtry Bayesa; - ochrona przed Blacklistingiem; - kwarantanna; - integracja z LDAP; - archiwizacja poczty w oparciu o polityki; - szyfrowanie poczty w oparciu o polityki (IBE); - raportowanie; - przechowywanie poczty na zewnętrznych zasobach; - konfiguracja HA; - tworzenie kopi zapasowej oraz jej odtwarzanie; **1.4. Wymagany zakres szkolenia FortiAuthenticator:** Szkolenie powinno obejmować co najmniej następujące zagadnienia: - wprowadzenie do FortiAuthenticator. - architektura rozwiązania. - instalacja i wstępna konfiguracja. - zarządzanie użytkownikami i grupami. - integracja z: ✓ Microsoft Active Directory, ✓ LDAP, ✓ RADIUS, ✓ TACACS+. - konfiguracja metod uwierzytelniania: ✓ hasła, ✓ tokeny sprzętowe i programowe, ✓ FortiToken, ✓ certyfikaty cyfrowe, ✓ FIDO2 (jeżeli wspierane przez wykorzystywaną wersję). - konfiguracja MFA. - zarządzanie certyfikatami: ✓ lokalny urząd certyfikacji,	

	✓ import i eksport certyfikatów, ✓ CSR, ✓ odwoływanie certyfikatów (CRL). - integracja z: ✓ FortiGate, ✓ FortiClient, ✓ FortiManager, ✓ FortiAnalyzer, ✓ innymi urządzeniami wykorzystującymi RADIUS/TACACS+. - portal użytkownika. - Single Sign-On (FSSO). - logowanie i raportowanie. - backup i odtwarzanie konfiguracji. - aktualizacja systemu. - diagnostyka i troubleshooting. **1.5. Pozostałe wymagania dotyczące szkoleń firmy Fortinet:** - liczba osób przewidzianych do każde szkolenie – min. 3 osoby; - poziom zaawansowania – średni; - minimalny czas trwania każdego ze szkoleń Fortinet – 2 dni robocze; - łączna liczba godzin szkoleniowych na każde szkolenie: minimum 12 godzin zegarowych; - sugerowany harmonogram - 2 kolejne dni robocze na każde szkolenie, w godzinach dostosowanych do standardowego dnia pracy (np. 9:00-16:00/16:30 z przerwami); - harmonogram szkoleń do uzgodnienia z Zamawiającym; - termin szkolenia – po uzgodnieniu z Zamawiającym. 1.5.1. Wykonawca zapewni: ✓ materiały szkoleniowe w języku polskim lub angielskim; ✓ instrukcje do laboratoriów; ✓ prezentacje; ✓ dokumentację techniczną; ✓ dostęp do środowiska laboratoryjnego na czas szkolenia; ✓ indywidualne środowisko laboratoryjne dla każdego uczestnika. 1.5.2. Forma szkolenia – online lub stacjonarne, obejmująca ćwiczenia praktycznie na środowisku testowym Wykonawcy, oraz: ✓ w przypadku szkolenia stacjonarnego poza siedzibą/miejscowość siedziby Zamawiającego, zapewnienie całodziennego wyżywienia oraz noclegu (dwa noclegi na dwa dni szkolenia); ✓ po zakończeniu szkolenia uczestnik otrzyma imienny certyfikat potwierdzający ukończenie szkolenia z zakresu administracji i obsługi urządzeń Fortinet® z każdego szkolenia niezależnie;	

	1.5.3. Wykonawca zapewni każdemu uczestnikowi możliwość kontaktu z trenerem (np. poprzez e mail) przez okres minimum 14 dni kalendarzowych po zakończeniu szkolenia, w celu uzyskania odpowiedzi na pytania dotyczące zakresu odbytego szkolenia; 1.5.4. Zamawiający nie wymaga szkolenia autoryzowanego;	

Część 2: **Szkolenie administratorów systemów informatycznych z AI realizowane na rzecz Rządowego Centrum Bezpieczeństwa**

L.p.	**Wymagania minimalne które musi spełnić proponowane szkolenie**	**Proponowane szkolenie spełnia/nie spełnia wymagań**
1	1.1. Zrozumienie specyficznego ryzyka związanego z AI w kontekście rządowym: - jak ryzyko AI różni się od tradycyjnego ryzyka IT i danych; - kategorie ryzyka AI: techniczne, operacyjne, reputacyjne i etyczne; - odpowiedzialność publiczna i postrzeganie ryzyka w rządzie. 1.2. Ramy zarządzania ryzykiem AI: - ramy Zarządzania Ryzykiem AI NIST (AI RMF); - ISO/IEC 42001:2023 — Standard Systemu Zarządzania AI; - inne wytyczne sektorowe i międzynarodowe (np. OECD, UNESCO). 1.3. Zagrożenia bezpieczeństwa dla systemów AI: - wrogie dane wejściowe, zatruwanie danych i inwersja modelu; - ujawnienie wrażliwych danych treningowych; - ryzyka związane z łańcuchem dostaw i modelami stron trzecich. 1.4. Zarządzanie, audyt i kontrola: - mechanizmy odpowiedzialności z udziałem człowieka; - audytowalne AI: dokumentacja, wersjonowanie i interpretowalność; - kontrole wewnętrzne, role nadzorcze i punkty kontrolne zgodności. 1.5. Ocena ryzyka i planowanie działań zaradczych: - tworzenie rejestrów ryzyka dla przypadków użycia AI; - współpraca z zespołami ds. zamówień, prawnymi i projektowania usług; - przeprowadzanie ocen przed wdrożeniem i po wdrożeniu. - Reagowanie na incydenty i odporność sektora publicznego: ✓ reagowanie na incydenty i naruszenia związane z AI; ✓ komunikacja z interesariuszami i społeczeństwem; ✓ wdrażanie praktyk zarządzania ryzykiem AI w podręcznikach cyberbezpieczeństwa. **2. Pozostałe wymagania dotyczące szkolenia;** - liczba osób wskazanych do szkolenie – min. 1 osoba; - poziom zaawansowania – średni; - tryb (online). 2.1. Wykonawca zapewni: - materiały szkoleniowe w języku polskim lub angielskim; - instrukcje do laboratoriów; - prezentacje; - dokumentację techniczną; - dostęp do środowiska laboratoryjnego na czas szkolenia (jeżeli tematy szkolenia tego wymagają); - indywidualne środowisko laboratoryjne dla każdego uczestnika szkolenia	SPEŁNIA/ NIE SPEŁNIA*

	(jeżeli tematy szkolenia tego wymagają); 2.2. Termin szkolenia – po uzgodnieniu z Zamawiającym; 2.3. Forma szkolenia – online, obejmująca ćwiczenia praktycznie na środowisku testowym Wykonawcy (jeżeli takie są wymagane przez Zamawiającego); 2.4. Po zakończeniu szkolenia uczestnik otrzyma imienny certyfikat potwierdzający ukończenie szkolenia z zakresu objętego szkoleniem; 2.5. Zamawiający nie wymaga szkolenia autoryzowanego;	

Część 3: **Szkolenie administratorów systemów informatycznych realizowane z systemów rodziny MS Windows na rzecz Rządowego Centrum Bezpieczeństwa**

L.p.	Wymagania minimalne które musi spełnić proponowane szkolenie	Proponowane szkolenie spełnia/nie spełnia wymagań
1	1.1. Wprowadzenie do usługi AD DS w Windows Server: - Active Directory – omówienie: - co nowego w Windows Server?; - co nowego w Active Directory?; - budowa logiczna usługi AD DS.; - budowa fizyczna usługi AD DS.; - działanie usługi AD DS. 1.2. Instalacja usługi AD DS w Windows Server: - wdrażanie usług AD DS; - wzorce operacji FSMO; - wdrażanie i klonowanie wirtualnych kontrolerów domeny; - wdrażanie kontrolerów domeny w środowisku Azure oraz synchronizacja z Entra ID. 1.3. Administrowanie AD DS: - graficzne konsole administracyjne; - narzędzia linii poleceń; - zarządzanie obiektami za pomocą Powershell; - typowe czynności administracyjne. 1.4. Replikacja bazy AD: - omówienie replikacji usług AD DS; - konfigurowanie lokacji AD DS. 1.5. Zabezpieczanie AD DS: - bezpieczeństwo kontrolerów domeny. 1.6. Monitorowanie i odzyskiwanie usług AD DS: - monitorowanie AD DS; - zarządzanie bazą danych AD DS.; - opcje tworzenia kopii zapasowych i odzyskiwania AD DS. 1.7. Wdrażanie polityk GPO: - wprowadzenie do zasad grupy; - wdrażanie i administrowanie obiektami GPO; - rozwiązywanie problemów z zastosowaniem obiektów zasad grupy. 1.8. Konfiguracja środowiska pracy użytkownika za pomocą zasad grupy: - szablony administracyjne;	SPEŁNIA/ NIE SPEŁNIA*

	- konfigurowanie przekierowania folderów i skryptów; - instalacja oprogramowania; - konfigurowanie preferencji zasad grup. **2. Pozostałe wymagania dotyczące szkoleń;** - liczba osób wskazanych do każde szkolenie – min. 1 osoba; - poziom zaawansowania – średni; - tryb (online). 2.1. Wykonawca zapewni: - materiały szkoleniowe w języku polskim lub angielskim; - instrukcje do laboratoriów; - prezentacje; - dokumentację techniczną; - dostęp do środowiska laboratoryjnego na czas szkolenia (jeżeli tematy szkolenia tego wymagają); - indywidualne środowisko laboratoryjne dla każdego uczestnika (jeżeli tematy szkolenia tego wymagają); 2.2. Termin szkolenia – po uzgodnieniu z Zamawiającym; 2.3. Forma szkolenia – online, obejmująca ćwiczenia praktycznie na środowisku testowym Wykonawcy (jeżeli takie są wymagane przez Zamawiającego); 2.4. Po zakończeniu szkolenia uczestnik otrzyma imienny certyfikat potwierdzający ukończenie szkolenia z zakresu objętego szkoleniem; 2.5. Zamawiający nie wymaga szkolenia autoryzowanego;	

3. Zobowiązujemy się, w przypadku wybrania przez Zamawiającego naszej oferty:
   1) zawrzeć umowę na realizację przedmiotu zamówienia, na warunkach określonych w SWZ, w terminie i miejscu wskazanym przez Zamawiającego,
   2) wykonać przedmiot zamówienia zgodnie z postanowieniami SWZ.
4. Przedkładając Zamawiającemu naszą ofertę oświadczamy, że zapoznaliśmy się z treścią SWZ, OPZ oraz projektowanymi postanowieniami umowy i akceptujemy je bez zastrzeżeń.
5. Akceptujemy Projektowane postanowienia umowy (stanowiące załącznik nr 2 do SWZ/odnośnie części w zakresie której złożyliśmy ofertę) i zobowiązujemy się, w przypadku wybrania naszej oferty, do zawarcia umowy o treści określonej w Projektowanych postanowieniach umowy w terminie wyznaczonym przez Zamawiającego.
6. Oświadczamy, że w przypadku wspólnego ubiegania się o udzielenie zamówienia ponosimy solidarną odpowiedzialność za wykonanie przedmiotu umowy.
7. Oświadczamy, że wykazując spełnienie warunków udziału w postępowaniu[2]:

   □ nie polegamy na potencjale udostępnionym przez podmiot udostępniający zasoby;

[2] właściwe zaznaczyć - X

□ polegamy na potencjale udostępnionym przez podmiot udostępniający zasoby, a w związku z powyższym wraz z ofertą składamy zobowiązanie podmiotu udostępniającego zasoby do oddania do dyspozycji niezbędnych zasobów lub inny podmiotowy środek dowodowy.

8. Oświadczamy, że informacje i dokumenty, zawarte w pliku *(wypełnić, jeśli dotyczy)*, tj. następujące elementy oferty: ....., stanowią tajemnicę przedsiębiorstwa w rozumieniu art. 11 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji i zastrzegamy, że nie mogą być udostępnione. Elementy oferty, o których mowa powyżej, zostały złożone w osobnym pliku i oznaczone **„Dokument stanowiący tajemnicę przedsiębiorstwa".**
9. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.[3]
10. Akceptujemy postanowienia: Regulaminu Platformy e-Zamówienia[4] i instrukcji użytkownika Platformy e-Zamówienia[5].
11. Oświadczamy, że zamierzamy powierzyć podwykonawcy/podwykonawcom (proszę wypełnić jeżeli dotyczy, w zakresie w jakim dane podwykonawcy są znane) następującą część zamówienia:

Część (zakres) przedmiotu zamówienia, który zamierzamy powierzyć podwykonawcy	Nazwa (firma) podwykonawcy (jeżeli jest znana)

12. Oświadczenie składane przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia (jeżeli dotyczy):

Oświadczamy, że część zamówienia, co do której Zamawiający wymagał wykazania się doświadczeniem opisanym w warunku udziału w postępowaniu, zostanie wykonana przez ten z podmiotów wspólnie ubiegających się o zamówienie, którego doświadczenie zostało wykazane na potwierdzenie spełnienia tego warunku udziału w postępowaniu.

W związku z powyższym podział zadań w ramach Wykonawców występujących wspólnie przedstawia poniższa tabela:

[3] W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (prosimy o usunięcie treści oświadczenia np. przez jego wykreślenie).

[4] Z zapisami regulaminu można zapoznać się pod adresem: https://edu.ezamowienia.gov.pl/pl/regulamin/#:~:text=Regulamin%20Platformy%20e-Zam%C3%B3wienia%201%20%C2%A71.%20Definicje%20u%C5%BCyte%20w,zamawiaj%C4%85cymi%20a%20wykonawcami.%20...%202%20%C2%A72.%20Postanowienia%20og%C3%B3lne

[5] Z zapisami instrukcji można zapoznać się pod adresem: https://ezamowienia.gov.pl/pl/instrukcje/

Zadanie	Podmiot realizujący zadanie

13. UWAGA - dotyczy tylko Wykonawców zagranicznych.

Oświadczamy, że wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego w odniesieniu do następujących towarów/usług *):

W takim przypadku należy uzupełnić następującą tabelkę:

Lp.	Nazwa (rodzaj) towaru lub usługi	Wartość towaru lub usługi bez VAT	Stawka VAT, która będzie miała zastosowanie
1			
2			

W przypadku braku wypełnienia tabeli powyżej - oświadczam, że złożenie oferty nie prowadzi do powstania obowiązku podatkowego po stronie Zamawiającego.

*) powstanie dodatkowego obowiązku podatkowego u Zamawiającego zachodzi jedynie w sytuacji, kiedy wystawiona faktura nie będzie zawierała kwoty podatku VAT (sytuacja taka może wynikać z takich okoliczności jak: - wewnątrzwspólnotowe nabycie towarów, - import usług lub towarów, - mechanizm odwróconego obciążenia podatkiem VAT, np. określone w ustawie o podatku od towarów i usług dostawy sprzętu elektronicznego) - tylko w takich przypadkach Wykonawca zobowiązany (i uprawniony) jest do wypełniania przedmiotowego oświadczenia.

W przypadku braku skreślenia/niewskazania żadnej z ww. treści oświadczenia, Zamawiający uzna, że wybór przedmiotowej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.

Do Formularza oferty dołączam następujące załączniki:

1. **Oświadczenie/a o spełnieniu warunków udziału w postępowaniu i braku podstaw do wykluczenia z postępowania** (w tym w zakresie przesłanek z art. 7 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego) odpowiednio dla wykonawcy i/lub wykonawcy wspólnie ubiegającego się o udzielenie zamówienia i/lub podmiotu udostępniającego zasoby;
2. Pełnomocnictwo do reprezentowania wykonawcy (jeżeli dotyczy);
3. Pełnomocnictwo do reprezentowania wykonawców wspólnie ubiegających się o zamówienie (jeżeli dotyczy);
4. Uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa (jeżeli dotyczy);

5. Oświadczenie podmiotu udostępniającego zasoby (jeżeli dotyczy);
6. ……..

Uwaga!

kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty upoważnionego przedstawiciela odpowiednio Wykonawcy/Wykonawcy wspólnie ubiegającego się o udzielenie zamówienia

Załącznik nr 4 do SWZ

Kancelaria Prezesa Rady Ministrów
Al. Ujazdowskie 1/3
00-583 Warszawa

Oświadczenie odpowiednio Wykonawcy,
Wykonawcy wspólnie ubiegającego się o zamówienie,
Podmiotu udostępniającego Wykonawcy niezbędne zasoby
(składane wraz z ofertą)

o spełnianiu warunków udziału w postępowaniu, w zakresie w jakim Wykonawca, Wykonawca wspólnie ubiegający się o zamówienie, Podmiot udostępniający Wykonawcy niezbędne zasoby, wykazuje spełnienie warunków udziału w postępowaniu i brak podstaw do wykluczenia z postępowania

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego przez Kancelarię Prezesa Rady Ministrów pn. „Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa w ramach 3 części:
Część 1 - Szkolenie administratorów systemów informatycznych z Fortinet® realizowane na rzecz Rządowego Centrum Bezpieczeństwa;
Część 2 - Szkolenie administratorów systemów informatycznych z AI realizowane na rzecz Rządowego Centrum Bezpieczeństwa;
Część 3 - Szkolenie administratorów systemów informatycznych realizowane z systemów rodziny MS Windows na rzecz Rządowego Centrum Bezpieczeństwa", nr TP-31/26

Będąc upoważnionym do reprezentacji:
☐ Wykonawcy,

☐ Wykonawcy wspólnie ubiegającego się o udzielenie zamówienia,

☐ Podmiotu udostępniającego Wykonawcy niezbędne zasoby[6]:

Nazwa/firma Wykonawcy/Podmiotu .....

Adres .....

Nazwa rejestru .....

Adres strony internetowej bezpłatnej i ogólnodostępnej bazy danych, z której Zamawiający może samodzielnie pobrać odpis z odpowiedniego rejestru, dotyczący Wykonawcy:
.....
...

I. Oświadczam, że na dzień składania ofert spełniam warunki udziału w powołanym postępowaniu określone przez Zamawiającego w rozdziale V SWZ.

[6] Proszę zaznaczyć właściwe i wpisać poniżej dane odpowiedniego podmiotu

II. Oświadczam, że na dzień składania ofert nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 pkt 1-6 ustawy pzp oraz art. 109 ust. 1 pkt 4 i 8-10 ustawy pzp.

III. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (Dz. U. poz. 835)[7].

IV. **Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia** z postępowania na podstawie art. ..... ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 lub 6 ustawy pzp oraz art. 109 ust. 1 pkt 4 i 8-10 ustawy pzp). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy pzp podjąłem następujące środki naprawcze[8]:.....
.....

V. Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

VI. **Oświadczamy,** że nasze dokumenty rejestrowe dostępne są w formie elektronicznej w ogólnodostępnej bazie danych, z której Zamawiający może pobrać samodzielnie:

□ **KRS nr….., nazwa rejestru i adres strony internetowej** ..... (należy podać jeżeli dotyczy);

□ **innego rejestru, nazwa rejestru i adres strony internetowej** ..... (należy podać jeżeli dotyczy);

□ nie dotyczy.

VII. *(Jeżeli Wykonawca będzie posługiwał się certyfikatem wypełnia niniejszy punkt oświadczenia)*

Oświadczam, że będziemy posługiwali się certyfikatem potwierdzającym udzielenie certyfikacji wykonawców zamówień publicznych. W związku z powyższym podaje:

a) numer i oznaczenie certyfikatu: .....

b) nazwę podmiotu certyfikującego, który wydał ten certyfikat: .....

c) okres ważności certyfikacji: .....

d) w zakresie których podstaw wykluczenia lub warunków udziału w postępowaniu Wykonawca będzie posługiwał się tym certyfikatem: .....

---

[7] Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, zwanej dalej „ustawą", z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:
1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy
3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 ze zm.), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ww. ustawy.

[8] Należy uzupełnić jeżeli dotyczy.

kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty upoważnionego przedstawiciela odpowiednio Wykonawcy/Wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/Podmiotu udostępniającego Wykonawcy zasoby)

Załącznik nr 5 do SWZ

Zobowiązanie innego podmiotu do oddania
do dyspozycji wykonawcy niezbędnych zasobów
(składane wraz z ofertą – jeżeli dotyczy)

Dotyczy: postepowania o udzielenie zamówienia publicznego prowadzonego przez Kancelarię Prezesa Rady Ministrów pn. „Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa w ramach 3 części:
Część 1 - Szkolenie administratorów systemów informatycznych z Fortinet® realizowane na rzecz Rządowego Centrum Bezpieczeństwa;
Część 2 - Szkolenie administratorów systemów informatycznych z AI realizowane na rzecz Rządowego Centrum Bezpieczeństwa;
Część 3 - Szkolenie administratorów systemów informatycznych realizowane z systemów rodziny MS Windows na rzecz Rządowego Centrum Bezpieczeństwa", nr TP-31/26

DANE PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY:

Nazwa /Firma: .....

Adres: .....

telefon: .....

e-mail: .....

Będąc upoważnionym do reprezentowania wskazanego podmiotu, oświadczam, że oddaję do dyspozycji Wykonawcy:

Nazwa /Firma Wykonawcy: .....

Adres: .....

określone poniżej zasoby, przez okres korzystania z nich przy wykonaniu powołanego zamówienia i oświadczam, że stosunek łączący mnie z Wykonawcą gwarantuje rzeczywisty dostęp Wykonawcy do tych zasobów:

1. Określenie zakresu zasobów dostępnych Wykonawcy od podmiotu udostępniającego zasoby:
   .....
2. Sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia:
   .....

3. Czy i w jakim zakresie podmiot, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą .....

kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty osoby (osób) upoważnionej do występowania w imieniu Podmiotu udostępniającego Wykonawcy zasoby

Załącznik nr 6 do SWZ

Kancelaria Prezesa Rady Ministrów
Al. Ujazdowskie 1/3
00-583 Warszawa

Oświadczenie

(składane na wezwanie Zamawiającego)

o przynależności lub braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2025 r. poz. 1714), z innym wykonawcą, który złożył odrębną ofertę bądź ofertę częściową w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie podstawowym pn. „Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa w ramach 3 części:
Część 1 - Szkolenie administratorów systemów informatycznych z Fortinet® realizowane na rzecz Rządowego Centrum Bezpieczeństwa;
Część 2 - Szkolenie administratorów systemów informatycznych z AI realizowane na rzecz Rządowego Centrum Bezpieczeństwa;
Część 3 - Szkolenie administratorów systemów informatycznych realizowane z systemów rodziny MS Windows na rzecz Rządowego Centrum Bezpieczeństwa", nr TP-31/26

Oświadczam/oświadczamy w imieniu:

……, że:

nazwa Wykonawcy, adres

☐ **<u>nie należę</u>** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, z innym wykonawcą, który złożył odrębną ofertę bądź ofertę częściową w tym postępowaniu *),

☐ **<u>należę</u>** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, do której należy następujący wykonawca/cy, którzy złożyli odrębną ofertę bądź ofertę częściową w tym postępowaniu *):

……

W związku z powyższym do oświadczenia załączam dokumenty lub informacje potwierdzające przygotowanie oferty, oferty częściowej w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej.

***) niepotrzebne skreślić**

kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty osoby (osób) upoważnionej do występowania w imieniu Wykonawcy

Załącznik nr 7 do SWZ

Kancelaria Prezesa Rady Ministrów

Al. Ujazdowskie 1/3

00-583 Warszawa

Oświadczenie Wykonawcy

O PRAWIDŁOWOŚCI I AKTUALNOŚCI PODMIOTOWYCH ŚRODKÓW DOWODOWYCH,

KTÓRE ZAMAWIAJĄCY POSIADA

Będąc upoważnionym do reprezentacji Wykonawcy:

Nazwa/firma Wykonawcy ……..

Adres ……,

na potrzeby postępowania o udzielenie zamówienia publicznego pn. „Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa w ramach 3 części:
Część 1 - Szkolenie administratorów systemów informatycznych z Fortinet® realizowane na rzecz Rządowego Centrum Bezpieczeństwa;
Część 2 - Szkolenie administratorów systemów informatycznych z AI realizowane na rzecz Rządowego Centrum Bezpieczeństwa;
Część 3 - Szkolenie administratorów systemów informatycznych realizowane z systemów rodziny MS Windows na rzecz Rządowego Centrum Bezpieczeństwa", nr TP-31/26,
na podstawie art. 127 ust. 2 pzp oświadczam, że złożone …… (np. wraz z ofertą) następujące podmiotowe środki dowodowe**:**

1) ……

2) ……

3) ……

są prawidłowe i nadal aktualne.

kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty upoważnionego przedstawiciela odpowiednio Wykonawcy/Wykonawcy wspólnie ubiegającego się o udzielenie zamówienia