SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego pn.:

Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd” w Gminie Pieńsk w ramach: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (DERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd”

Spis treści

I ZAMAWIAJĄCY

Gmina Pieńsk, ul. Bolesławiecka 29, 59-930 Pieńsk

Niniejszy dokument określa minimalne wymagania dla zamówienia z zakresu cyberbezpieczeństwa w ramach realizacji projektu „Cyberbezpieczny Samorząd" dofinansowanego w formie grantu z programu Fundusze

Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa".

Postępowanie prowadzone jest zgodnie z postanowieniami ustawy prawo zamówień publicznych z dnia 11 września 2019 r. (dz.u. z 2024 r. poz. 1320) oraz aktów wykonawczych wydanych na jej podstawie.

Niniejsze postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, w którym w odpowiedzi na ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani Wykonawcy, a następnie Zamawiający wybiera najkorzystniejszą ofertę bez przeprowadzenia negocjacji (art. 275 pkt 1 ustawy Pzp). Zamawiający nie przewiduje możliwości wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji (art. 275 pkt 2 ustawy Pzp).

Zamawiający w okresie 3 lat od dnia udzielenia zamówienia podstawowego, dotychczasowemu wykonawcy nie przewiduje udzielenia zamówienia polegającego na powtórzeniu podobnych usług.
Zamawiający nie dopuszcza składania ofert wariantowych.
Zamawiający nie przewiduje wymagań wskazanych w art. 96 ust. 2 pkt 2 ustawy Pzp.
Zamawiający nie przewiduje wymagań wskazanych w art. 94 ustawy Pzp.
Zamawiający nie przewiduje zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.
Zamawiający nie wymaga przeprowadzenia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy Pzp.
Zamawiający nie przewiduje rozliczenia między Zamawiającym a Wykonawcą w walutach obcych.
Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
Zamawiający nie wymaga obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań zgodnie z art. 60 i art. 121 ustawy Pzp.
Zamawiający nie przewiduje zawarcia umowy ramowej
Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230 ustawy Pzp.
Zamawiający nie stawia wymogu lub możliwości złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93 ustawy Pzp.

Wykonawca jest związany ofertą do dnia 22-05-2025 r. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa w SWZ, Zamawiający przed upływem terminu związania ofertą, zwróci się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego

terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni. Przedłużenie terminu związania ofertą, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

Zamawiający nie wymaga wniesienia wadium ani zabezpieczenia należytego wykonania umowy.

II Definicje

Zamawiający dokonał opisu przedmiotu z wykorzystaniem następujących definicji:

Lp.	Termin	Definicje
1.	OPZ	Opis przedmiotu zamówienia
2.	Umowa	Należy przez to rozumieć umowę zawartą między zamawiającym a jednym lub większą liczbą wykonawców, której celem jest ustalenie warunków dotyczących zamówień, jakie mogą zostać udzielone w danym okresie, w szczególności cen i, jeżeli zachodzi taka potrzeba, przewidywanych ilości
3.	Zamawiający	Należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, obowiązaną na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych do jej stosowania.
4.	Wykonawca	należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która oferuje na rynku wykonanie robót budowlanych lub obiektu budowlanego, dostawę produktów lub świadczenie usług lub ubiega się o udzielenie zamówienia, złożyła ofertę lub zawarła umowę w sprawie zamówienia publicznego.

III Wartość zamówienia

1. Szacunkowa wartość zamówienia nie przekracza wyrażoną w złotych równowartość kwoty określonej w przepisach wydanych na podstawie ustawy prawo zamówień publicznych z dnia 11 września 2019 r. (dz.u. z 2024 r. poz. 1320).

IV Opis przedmiotu zamówienia

1. Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych

110 stacji komputerowych w 7 jednostkach

A. Podstawowe wymagania w zakresie oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej:

- Dostarczone licencje na oprogramowanie są bezterminowe, wsparcie nie przekraczające daty 30.06.2026 r.
- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
- Oprogramowanie współpracuje z serwerem SQL Server 2019, SQL Server 2017, SQL Server 2016 SP3, SQL Server 2014 SP3, Oracle 19c, Oracle 12c R2.
- Oprogramowanie serwera aplikacji umożliwia wysyłanie powiadomień mailowych.
- Oprogramowanie posiada system ról, dzięki któremu jest możliwe przypisywanie wybranych grup stanowisk do poszczególnych użytkowników konsoli.
- Wszelkie raporty, zestawienia oraz funkcje grupowe obejmują wtedy tylko w/w przypisane grupy stanowisk.
- Oprogramowanie realizuje zarządzanie wszystkimi modułami systemu z poziomu tej samej konsoli zarządzającej.
- Oprogramowanie agenta realizuje wszystkie wymagane funkcjonalności z poziomu jednej instancji usługi lub procesu bez wykorzystywania aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
- Oprogramowanie pozwala export do plików w formacie xls/xlsx dowolnego widoku konsoli administracyjnej.
- Oprogramowanie pozwala zarządzać z jednej konsoli zarówno stacjami klienckimi, serwerami jak i urządzeniami mobilnymi z systemami operacyjnymi Android oraz iOS.
- Oprogramowanie, niezależnie od ilości funkcjonalności lub zarządzanych urządzeń końcowych działa w oparciu o 1 oprogramowanie typu Agent na urządzeniu końcowym.
- Oprogramowanie posiada architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta.
- Oprogramowanie działa poprawnie na wymaganiach sprzętowych:

Wymagania dla serwera:

- procesor 2 rdzenie;

- 8 GB wolnej pamięci;

- karta sieciowa 1 Gigabit;

- przestrzeń instalacyjna: 5 GB;

- Serwer OS - od Windows Server 2016 (64-Bit);

- Baza Danych - od SQL Server 2014 SP3;

Wymagania dla stacji klienckiej:

- od Intel Pentium IV procesor z 1GHz;

- od 256 MB wolnej pamięci RAM;

- od 200 MB wolnego miejsca na dysku twardym;

- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
- Oprogramowanie umożliwia dystrybucję dowolnego oprogramowania, nie tylko paczek MSI, ale również takich jak InnoSetup, InstallShield i inne.
- Oprogramowanie umożliwia automatyzowanie instalatorów wraz z możliwością customizowania instalatorów w taki sposób, żeby można było nadpisywać pola opisowe, zmieniać dowolne wartości, w tym miejsce zapisu na dysku na urządzeniu końcowym.
- Oprogramowanie umożliwia administratorowi zautomatyzowanie procesu instalacji, w taki sposób, by nagrany został cały proces instalacji w taki sposób, by w momencie instalacji na urządzeniu końcowym nie było wymagane podanie jakichkolwiek opcji.
- Oprogramowanie musi umożliwiać zautomatyzowania zdalnej instalacji dowolnego oprogramowania w taki sposób, by oprogramowanie można było zainstalować zdalnie w trybie cichym (Silent Mode) lub graficznym.
- Oprogramowanie musi umożliwiać dodawanie takich opcji w instalatorach jak:

- blokowanie klawiatury i myszki;

- zmiany w ustawieniach w rejestracji na stacjach klienckich;

- działania na plikach I folderach na stacji klienckiej;

- dodanie skryptu np. w PowerShellu;

- zatrzymanie/wznowienie usług oraz procesów na stacji klienckiej.

- Zdalna dystrybucja oprogramowania musi wykorzystywać natywną inteligencję instalatora. Nie może wykorzystywać Snapshotingu.
- Zdalna dystrybucja oprogramowania musi mieć opcje Schedullingu:

- w zadanym przedziale czasowym;

- wprowadzenie cykliczności (np. wybrany dzień tygodnia o wybranej godzinie);

- połączenie dwóch powyższych;
- na żądanie w danym momencie;

- Oprogramowanie musi umożliwiać wzbudzanie stacji klienckich metodą Wake-On-LAN.
- Oprogramowanie musi umożliwiać administratorowi podgląd co do Statusu danego zadania per maszyna w czasie rzeczywistym, a w przypadku błędu w wykonaniu - zwrócić informację co było przyczyną błędu.
- W przypadku dokupienia nowych funkcjonalności/modułów oprogramowania, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
- W przypadku zwiększenia ilości zarządzanych maszyn w dowolnym momencie, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
- Oprogramowanie musi umożliwiać zdalną dystrybucję oprogramowania z jednej konsoli zarówno na stacjach klienckich (jak PC I laptop/notebook) jak i urządzeniach mobilnych z systemem Android.
- Oprogramowanie dostarczy administratorowi informacji o dacie ostatniego uruchomienia aplikacji na stacji klienckiej PC per każda stacja kliencka.
- Dystrybucja agentów na stacjach klienckich musi być możliwa zarówno w sposób automatyczny jak i ręczny.
- Oprogramowanie umożliwia integrację z Active Directory (AD) oraz pobranie informacji z AD i automatyczne zarejestrowanie urządzeń z AD w serwerze.
- Zarówno w przypadku stacji klienckich PC jak I urządzeń mobilnych z systemem Android, oprogramowanie musi umożliwiać administratorowi dostarczenie użytkownikowi końcowemu interfejsu typu self-service, w którym będzie miał listę dostępnych instalatorów z możliwością ich dociągnięcia i zainstalowania; Musi istnieć możliwość automatycznej personalizacji takiej listy per grupa lub konkretne urządzenie końcowe.
- Oprogramowanie musi posiadać otwarte API do integracji z zewnętrznymi serwerami, np. poprzez Web Service'y.
- Oprogramowanie musi umożliwiać również tworzenie własnych skryptów, które następnie można automatycznie instalować na urządzeniach końcowych, typu stacja kliencka.
- W przypadku automatycznej zdalnej instalacji oprogramowania na stacjach klienckich, oprogramowanie musi dać opcje tworzenia listy oprogramowania zależnego, tzn. w przypadku gdy do poprawnego działania aplikacja X wymaga instalacji aplikacji Y, Oprogramowanie musi dawać opcję ustalenia listy takiego oprogramowania zależnego na poziomie konfiguracji aplikacji X z poziomu konsoli. W przypadku dystrybucji aplikacji X, gdy na stacji klienckiej nie będzie zainstalowana aplikacja Y, serwer automatycznie wypchnie na tą stację paczkę instalacyjną aplikacji Y.

- Oprogramowanie musi dawać administratorowi możliwość przypisywania wykonywania zadań zarówno na urządzeniach końcowych spełniających wybrane warunki dynamiczne (np. wolne miejsce na dysku C, wersja systemu operacyjnego itp.), jak i urządzeniach przypisanych do konkretnych grup, jak w AD.
- Oprogramowanie musi posiadać środowisko skryptowe, umożliwiające tworzenie własnych skryptów i w łatwej dystrybucji skryptów z poziomu konsoli.
- Oprogramowanie wspiera MsSQL-Server (również w wersji Express).
- Oprogramowanie posiada konsolę zarządzającą jako część oprogramowania (nie tylko interfejs webowy).
- Oprogramowanie posiada Agenta dla systemów klienckich Windows od Windows oraz Windows Server.
- Oprogramowanie wspiera więcej niż jeden serwer-repozytorium (DIP-Server).
- Oprogramowanie wspiera PXE-Relay.
- Oprogramowanie wspiera WakeUp-Points.
- Oprogramowanie posiada możliwość integracji z Active Directory.
- Oprogramowanie obsługuje niewielką przepustowością łącza dla kontroli agentów i przesyłania informacji o statusach.
- Oprogramowanie umożliwia indywidualną synchronizację pomiędzy pojedynczymi serwerami repozytorium (ograniczenie czasowe i przepustowości łącza).
- Oprogramowanie posiada dostęp read-only do AD, bez rozszerzeń schematu
- Oprogramowanie umożliwia wybudzanie stacji klienckich Wake-On-LAN.
- Oprogramowanie wspiera zadania/Joby Push i Pull (łącznie z Shutdown).
- Oprogramowanie umożliwia komunikację bez konieczności zestawiania połączenia VPN z urządzeniami, które są poza siecią poprzez bramkę Proxy instalowaną w DMZ. Bramka Proxy musi stanowić integralną część Oprogramowania. Komunikacja pomiędzy bramką a agentem, jak i bramką a serwerem musi odbywać się poprzez HTTPS.
- Oprogramowanie obsługuje niewielką przepustowością łącza dla kontroli agentów i przesyłania informacji o statusach.
- Oprogramowanie umożliwia indywidualną synchronizację pomiędzy pojedynczymi serwerami repozytorium (ograniczenie czasowe i przepustowości łącza).
- Oprogramowanie posiada dostęp read-only do AD, bez rozszerzeń schematu
- Oprogramowanie umożliwia wybudzanie stacji klienckich Wake-On-LAN.
- Oprogramowanie wspiera zadania/Joby Push i Pull (łącznie z Shutdown).
- Oprogramowanie umożliwia komunikację bez konieczności zestawiania połączenia VPN z urządzeniami, które są poza siecią poprzez bramkę Proxy instalowaną w DMZ. Bramka Proxy musi stanowić integralną część Oprogramowania. Komunikacja pomiędzy bramką a agentem, jak i bramką a serwerem musi odbywać się poprzez HTTPS.
- Oprogramowanie umożliwia wysyłanie polecenia w trybie "Push".
- Oprogramowanie umożliwia wysyłanie polecenia w trybie "Pull".

- Oprogramowanie umożliwia wysyłanie polecenia w trybie "shutdown".
- Oprogramowanie pozwala na indywidualną interakcję użytkownika w trakcie wykonywania zadania uruchomionego przez administratora w trybach: opóźnienie, odmowa, przypomnienie o instalacji.
- Oprogramowanie umożliwia wysyłanie polecenia Wake-on LAN.
- Oprogramowanie umożliwia automatyczne generowanie i wysyłanie powtarzających się zadań (recurring Jobs).
- Oprogramowanie umożliwia uruchomienie zadania z poziomu użytkownika końcowego poprzez Kiosk samoobsługowy SelfService (dostępny przez Web).
- Zadania mogą być inicjowane z poziomu aplikacji selfservice - konsoli Webowej.
- Zawartość aplikacji SelfService (Kiosku) może być definiowana zarówno per User/Grupa Userów jak i per PC/Organisation Unit.
- Oprogramowanie umożliwia dystrybucji patchy Windows bez WSUS.
- Oprogramowanie umożliwia triggerowanie z poziomu WSUS.
- Oprogramowanie umożliwia obsługę systemów operacyjne Microsoft — Windows Server 2008, Windows 7, Windows 8, Windows 10, Windows 11, Windows Server 2008R2, Windows Server 2012, Windows Server 2019 z natywną instalacją.
- Producent oprogramowania zapewnia stały dostęp do bazy danych z poprawkami Microsoft - baza jest dostępna dla Klienta z poziomu konsoli oprogramowania w dniu jej opublikowania przez Microsoft.
- Oprogramowanie umożliwia określenie ścisłych wymagań czasowych dla instalacji poprawek Microsoft i te wymagania kontrolować. Oprogramowanie nie wymaga ingerencji w reguły eksploatacji serwerów, a mimo to zapewnia ich odpowiednio szybkie zamknięcie w razie luk w zabezpieczeniach.
- Oprogramowanie pozwala administratorowi zarządzać aktualizacją systemów: możliwość sprawdzania tylko pod kątem brakujących poprawek i czy poprawki mają być od razu instalowane. Poprawki mogą być zatwierdzane automatycznie lub ręcznie. Oprogramowanie pozwala także ustalać reguły dla różnych grup w systemie IT.
- Oprogramowania pozwala by metodą drag and drop w środowisku zgodnym z MMC określać, w jakich systemach mają być instalowane poprawki. W taki sam sposób definiowane są również automatyczne instalacje i sytuacje, w których administrator ma być wcześniej pytany o zgodę. Oprogramowanie automatycznie pobiera wszystkie poprawki Microsoft i na żądanie automatycznie je rozprowadza w infrastrukturze Klienta zgodnie z wytycznymi administratora kreator skryptów, konfiguracji pakietów i autmatyzacja dowolnych procesów / Automate i Package Studio.
- Oprogramowanie pozwala na tworzenie plików transformacji (MST), które umożliwiają niezawodne dopasowanie do każdego MSI.
- Oprogramowanie pozwala na tworzenie kreatora instalacji dla dowolnej aplikacji - nie wymaga paczki MSI.

- Oprogramowanie pozwala tworzyć pakiety instalacyjne, gdzie w ramach procesu można zainstalować "n" aplikacji lub wykonać szereg dodatkowych funkcji związanych np. z inwentaryzacją.
- Oprogramowanie obsługuje wszystkie powszechnie dostępne na rynku systemy operacyjne Microsoft - Windows Vista i Server 2008, Windows 7, Windows 8, Windows10, Windows 11, Windows Server 2008R2, Windows Server 2012 i Windows 2019.
- Oprogramowanie umożliwia tworzenie plików sterujących (transform).
- Oprogramowanie pozwala na automatyzacje niemal każdego procesu wykonywanego ręcznie na komputerze.
- Oprogramowania pozwala na proste tworzenie skryptów metodą drag and drop.
- Oprogramowanie zawiera standardowy zestaw poleceń.
- Oprogramowanie posiada możliwość sterowania również interfejsami niezgodnymi ze standardem (np. Java).
- Oprogramowanie posiada pomoc kontekstową.
- Oprogramowanie posiada tryb testowy step by step.

B. Szczegółowe wymagania w zakresie oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej:
   - Monitorowanie zużycia energii przez urządzenia w sieci.
   - Generowanie raportów o zużyciu energii.
   - Automatyczne wykrywanie i identyfikacja oprogramowania zainstalowanego na urządzeniach.
   - Gromadzenie szczegółowych informacji o oprogramowaniu, takich jak nazwa, wersja, wydawca, data instalacji i licencja.
   - Możliwość ręcznego dodawania oprogramowania do inwentaryzacji.
   - Aktualizacja informacji o oprogramowaniu w czasie rzeczywistym.

2. Oprogramowanie przeciwdziałające wyciekowi danych

Oprogramowanie na licencji wieczystej z wsparciem nie przekraczającym 30.06.2026 r. 110 stanowisk.

Minimalne wymagania w zakresie oprogramowania przeciwdziałającego wyciekowi danych

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11 z najnowszymi aktualizacjami.

2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.

3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.

4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.

5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.

6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.

7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.

8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.

9. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.

10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.

11. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.

12. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.

13. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.

14. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.

15. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:

- Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
- Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.

16. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.

17. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:

a. logowanie oraz wylogowanie użytkownika,

b. włączenie oraz wyłączenie stacji roboczej,

c. blokada oraz odblokowanie stacji roboczej,

d. przejście w stan bezczynności stacji roboczej.

18. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie zbliżonym do rzeczywistego.

19. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.

20. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.

21. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.

22. Serwer musi posiadać możliwość wysłania alertów co najmniej za pośrednictwem wiadomości email oraz za pomocą SIEM/SYSLOG.

23. Serwer administracyjny musi posiadać możliwość konfiguracji cyklicznych raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.

24. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.

25. Raporty muszą być generowane do pliku PDF i/lub XLS, zapisywane w lokalizacji na serwerze lub na wskazany adres(y) e-mail.

26. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania, ale również umożliwiać jego zmianę na serwer klienta.

27. Serwer administracyjny musi posiadać możliwość wyszukiwania plików w oparciu o ich zawartość, co najmniej o:

a) numery kart kredytowych,

b) numer PESEL,

c) numer polskiego dowodu osobistego,

d) polski numer paszportu,

e) wyrażenia regularne,

f) określone ciągi znaków,

g) numer IBAN.

28. Weryfikacja zawartości pliku powinna odbywać się w czasie rzeczywistym.

29. System musi posiadać możliwość importu własnych słowników do klasyfikowania danych.

30. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych od jakich plik zostanie sklasyfikowany.

31. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:

a) audyt i logowanie wiadomości e-mail,

b) audyt i logowanie operacji na plikach.

32. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi.

33. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:

a) Bezpieczeństwo danych:

• Przegląd informacji o incydentach bezpieczeństwa.

• Przegląd danych przychodzących.

• Przegląd danych wychodzących.

• Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.

• Podłączane/odłączane urządzenia przenośne.

b) Produktywność:

• Przegląd informacji na temat produktywności użytkowników.

• Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.

c) Eksploatacja sprzętu:

• Przegląd informacji na temat eksploatacji sprzętu komputerowego.

• Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.

• Eksploatacja drukarek.

• Eksploatacji sieci.

34. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.

35. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.

36. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt:

• plików przenoszonych na nośniki USB i inne urządzenia przenośne,

• plików przesłanych za pomocą wiadomości e-mail,

• plików przesłanych za pomocą poczty webowej,

• plików przesłanych do Internetu,

• plików wysłanych za pomocą komunikatorów,

• plików przesłanych na dyski chmurowe,

• analiza sposobu korzystania z aplikacji,

• analiza korzystania z Internetu,

• analiza wykorzystania portali do poszukiwania pracy

3. Oprogramowanie do szyfrowania danych

4. Utrzymanie systemów teleinformatycznych

Usługi stałego wsparcia technicznego (II linia wsparcia IT)

Przedmiotem zamówienia jest świadczenie usług stałej opieki informatycznej dla Zamawiającego, obejmujących w ilości 120 godzin oraz w okresie 12 miesięcy:

- pomoc zdalna w rozwiązywaniu problemów z serwerami i oprogramowaniem serwerowym;
- monitorowanie dostępności serwerów i usług;
- reagowanie na problemy związane z dostępnością serwerów;
- zarządzanie zmianami i wersjami oprogramowania serwerowego;
- instalacja i konfiguracja nowego oprogramowania i sprzętu;

- zarządzanie patchami i aktualizacjami oprogramowania;
- backup i odzyskiwanie danych;
- monitorowanie wydajności systemów i aplikacji;
- diagnozowanie i rozwiązywanie problemów z wydajnością;
- zarządzanie konfiguracją systemów i aplikacji;
- automatyzacja rutynowych zadań operacyjnych;
- analiza i interpretacja logów systemowych i aplikacji;
- reagowanie na alerty bezpieczeństwa generowane przez SIEM;
- analiza trendów i przewidywanie przyszłych problemów;
- wdrażanie i zarządzanie kontenerami i usługami mikrousług;
- konfiguracja i zarządzanie sieciami wirtualnymi;
- zarządzanie certyfikatami SSL/TLS;
- wdrażanie zasad bezpieczeństwa i konfiguracji firewalli;
- audyt konfiguracji i zabezpieczeń systemów;
- przeprowadzanie testów penetracyjnych i ocen ryzyka;
- zarządzanie użytkownikami i uprawnieniami;
- zarządzanie bazami danych (backup, tuning, aktualizacje);
- zarządzanie środowiskami deweloperskimi, testowymi i produkcyjnymi;

- wsparcie dla procesów CI/CD (Continuous Integration/Continuous Deployment);
- doradztwo w zakresie architektury systemów i aplikacji;
- optymalizacja kosztów usług chmurowych;
- zarządzanie kluczami szyfrowania i dostępem do danych wrażliwych;
- planowanie i testowanie ciągłości działania (DR/BCP);
- zarządzanie incydentami bezpieczeństwa i reagowanie na nie;
- konsultacje w zakresie najlepszych praktyk DevOps i bezpieczeństwa IT;
- analiza przyczynowa (Root Cause Analysis) dla incydentów IT;
- zarządzanie dokumentacją techniczną i operacyjną;
- wsparcie przy migracjach systemów i aplikacji;
- ocena zgodności z wymaganiami regulacyjnymi i standardami branżowymi;
- szkolenia użytkowników i personelu technicznego w zakresie obsługi systemów;
- monitorowanie zagrożeń w cyberprzestrzeni i aktualizacja zabezpieczeń;
- zarządzanie konfiguracją sieci i urządzeń sieciowych;
- ocena skuteczności zaimplementowanych środków bezpieczeństwa;
- wsparcie dla procesów skalowania infrastruktury IT;
- analiza potrzeb biznesowych i doradztwo technologiczne;
- optymalizacja procesów biznesowych za pomocą technologii IT;

- przeglądy architektury systemów pod kątem najlepszych praktyk i zaleceń;
- wsparcie w zakresie integracji systemów i aplikacji;
- zarządzanie środowiskami wirtualnymi i chmurowymi;
- ocena wykorzystania zasobów IT i rekomendacje dotyczące optymalizacji;
- zarządzanie zmianą w infrastrukturze IT i procesach operacyjnych.

Zadania będą realizowane selektywnie i niezwłocznie na każde wezwanie Zamawiającego w godzinach 8:00 – 16:00 oraz w przypadku problemów krytycznych, przez całą dobę.

5. Audyty bezpieczeństwa - Testy penetracyjne

Testy penetracyjne infrastruktury 5 dni

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia. Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:

- wykonanie skanowań z wykorzystaniem wbudowanych szablonów;
- skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi);
- weryfikacje domyślnych haseł według zadanego słownika;
- skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy i aplikacje) oraz weryfikację uprawnień zadanego użytkownika;

- ustawienia harmonogramu skanowań;
- możliwość porównania wyników poszczególnych skanowań
- możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (w tym HTML, CVS i XML);
- możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności i możliwość sortowania po IP i podatnościach.

Aplikacji do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:

- przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
- przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;
- dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
- wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
- tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
- precyzyjna konfiguracja reguł przechwytywania wiadomości;
- możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;
- pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
- żądania i odpowiedzi dostępne w edytorze http;

- narzędzie do ręcznej edycji i ponownego wstawiania żądań;
- narzędzie do analizy statystycznej tokenów sesji;
- możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz powrót do zapisanego miejsca;
- biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;
- możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;
- skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
- możliwość analizy docelowej aplikacji internetowych.
- narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.

Potencjał osobowy przedstawia się poprzez posiadanie przez osoby testujące łącznie takie certyfikaty jak: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity), eCPPT (eLearnSecurity). Skanowania nie mogą być realizowane tylko z wykorzystaniem narzędzi automatycznych, konieczna jest manualna weryfikacja podatności znalezionych w testach automatycznych. Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.

W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

1. Rekonesans.

1. Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję w celu stworzenia potencjalnej bazy loginów i haseł.

2. Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi).

3. zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych.

4. Sprawdzenie występowania w wyciekach znalezionych loginów.

2. Enumeracja zasobów.

1. Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz z określeniem ich wersji) działających w ramach usług.

2. Skanowanie publicznej infrastruktury.

3. Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.

4. Sprawdzenie udostępnionych w sieci wewnętrzej plików i folderów w szczególności pod kątem występowania danych wrażliwych.

3. Eksploitacja.

1. Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.

2. Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) – po uzgodnieniu z Zamawiającym.

3. Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).

4. Eskalacja uprawnień.

1. Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.

2. Rozpoznanie zasobów wewnętrznych.

5. Raport z testu penetracyjnego.

Wykonawca dostarczy raport zawierający:

1. Podsumowanie dla kierownictwa.

2. Opis zakresu wykonanych prac.

3. Wyłączenia z testów jeżeli były.

4. Listę danych zebranych w trakcie rekonesansu (w tym listę zidentyfikowanych adresów IP w sieci wewnętrznej).

5. Listę znalezionych podatności wraz z określoną dla niej waga zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.

6. Szczegółowy opis znalezionych podatności.

7. Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.

6. Szkolenia powiązane z testami socjotechnicznymi

Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami:

1. Przygotowanie kampanii socjotechnicznej;

a. wybór i zakup przez Wykonawcę domeny (łudząco podobnej do domeny Zamawiającego), która zostanie wykorzystana do kampanii socjotechnicznej;

b. opracowanie bazy mailingowej pracowników objętych kampanią socjotechniczną oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłośliwy kod pozwalający na mierzenie efektów kampanii;

c. wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);

d. wsparcie w zakresie dodania domeny wybranej do przeprowadzenia kampanii socjotechnicznej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców).

2. Przygotowanie spreparowanych zasobów służących wyłudzaniu informacji:

a. serwer strony www z bazą danych powiązany z domeną, która została zakupiona w celu przeprowadzenia kampanii socjotechnicznej;

b. wykonanie kopii strony internetowej Zamawiającego i umieszczenie jej pod spreparowanym adresem;

c. wygenerowanie niezbędnych certyfikatów SSL;

d. przygotowanie spreparowanego aktywnego dokumentu PDF, wyposażonego w autorski, niezłośliwy skrypt, którego celem jest zebranie informacji o użytkownikach, którzy dokonali otwarcia pliku PDF i uruchomienia niezłośliwego skryptu (w prawdziwej kampanii byłoby to złośliwe oprogramowanie);

e. utworzenie nowej podstrony, na której umieszczony zostanie spreparowany plik PDF;

f. przygotowanie konta mailowego, którego celem jest podszycie się pod jedną z osób wtajemniczonych w prowadzone testy phishingowe;

g. przygotowanie treści wiadomości e-mail i wyposażenie jej w mechanizmy pozwalające na przeprowadzenie tzw. detekcji umiejscowienia (uzyskanie adresu IP potencjalnej „ofiary").

3. Przeprowadzenie kampanii socjotechnicznej (wysłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej).

4. Wykonanie raportu z testu socjotechnicznego w języku polskim.

5. Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa, ukierunkowanego na omówienie wyników kampanii socjotechnicznej oraz co najmniej:

a. wprowadzenie do cyberbezpieczeństwa:

- czym jest cyberbezpieczeństwo;
- dlaczego cyberbezpieczeństwo jest ważne;
- kluczowe zagadnienia związane z cyberbezpieczeństwem;
- przegląd statystyk i trendów w cyberbezpieczeństwie.

b. typy zagrożeń w cyberprzestrzeni:

- malware (wirusy, trojany, robaki itp.);
- ataki typu phishing i spear phishing;
- ataki DDoS;
- ataki ransomware;
- zagrożenia związane z sieciami społecznościowymi.

c. zasady bezpieczeństwa i praktyki:

- zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
- zasady bezpieczeństwa e-mail;
- bezpieczeństwo w sieciach bezprzewodowych;
- bezpieczne przeglądanie internetu;
- backup i odzyskiwanie danych.

d. reagowanie na incydenty i planowanie awaryjne:

- jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
- zasady reagowania na incydenty;
- planowanie awaryjne i kontynuacja działalności;
- Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

Czas trwania szkolenia przewidziano na co najmniej dwie grupy po 4 godziny robocze każda z uwzględnieniem przerw 15 minut w każdym szkoleniu. Po szkoleniu Wykonawca udostępni co najmniej 30 minut na pytania i odpowiedzi uczestników.

7. Szkolenie z cyberbezpieczeństwa dla kadry administracyjnej

Szkolenie dla pracowników administracyjnych w zakresie cyberbezpieczeństwa

Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników administracyjnych.

Szkolenie stacjonarne lub online z zakresu cyberbezpieczeństwa skierowane do pracowników administracyjnych, obejmujące co najmniej następujące obszary:

a. wprowadzenie do cyberbezpieczeństwa:

- czym jest cyberbezpieczeństwo;
- dlaczego cyberbezpieczeństwo jest ważne;
- kluczowe zagadnienia związane z cyberbezpieczeństwem;
- przegląd statystyk i trendów w cyberbezpieczeństwie.

b. typy zagrożeń w cyberprzestrzeni:

- malware (wirusy, trojany, robaki itp.);
- ataki typu phishing i spear phishing;
- ataki DDoS;
- ataki ransomware;
- zagrożenia związane z sieciami społecznościowymi.

c. zasady bezpieczeństwa i praktyki:

- zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
- zasady bezpieczeństwa e-mail;
- bezpieczeństwo w sieciach bezprzewodowych;

- bezpieczne przeglądanie internetu;
- backup i odzyskiwanie danych.

d. reagowanie na incydenty i planowanie awaryjne:

- jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
- zasady reagowania na incydenty;
- planowanie awaryjne i kontynuacja działalności;
- Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

Przewiduje się, że szkolenie potrwa łącznie minimum 8 godzin roboczych, rozłożonych na co najmniej 1 dzień. Zajęcia będą organizowane w dwóch grupach szkoleniowych, gdzie każda grupa będzie miała 4 godziny zajęć dziennie. Dodatkowo, każda sesja będzie obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

8. Szkolenie z cyberbezpieczeństwa dla kadry informatycznej

Szkolenie dla pracowników IT w zakresie cyberbezpieczeństwa

Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa:

Szkolenie z cyberbezpieczeństwa dla pracowników IT.

Indywidualne warsztaty online z zakresu cyberbezpieczeństwa skierowane do administratorów sieci teleinformatycznej, obejmujące co najmniej następujące obszary:

1. Wprowadzenie do cyberbezpieczeństwa:
   - Czym jest cyberbezpieczeństwo?
   - Dlaczego cyberbezpieczeństwo jest ważne?
   - Kluczowe zagadnienia związane z cyberbezpieczeństwem.
   - Przegląd statystyk i trendów w cyberbezpieczeństwie.
2. Typy zagrożeń w cyberprzestrzeni:
   - Malware (wirusy, trojany, robaki itp.)
   - Ataki typu phishing i spear phishing
   - Ataki DDoS
   - Ataki ransomware
   - Zagrożenia związane z sieciami społecznościowymi.
3. Zasady bezpieczeństwa i praktyki:
   - Zarządzanie hasłami i uwierzytelnianie wieloskładnikowe
   - Zasady bezpieczeństwa e-mail
   - Bezpieczeństwo w sieciach bezprzewodowych

- Bezpieczne przeglądanie internetu
- Backup i odzyskiwanie danych

4. Bezpieczeństwo systemów i sieci

- Zasady bezpieczeństwa systemów operacyjnych
- Bezpieczeństwo sieci i firewall
- Wprowadzenie do VPN
- Bezpieczeństwo urządzeń IoT
- Bezpieczeństwo w chmurze

5. Reagowanie na incydenty i planowanie awaryjne

- Jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem
- Zasady reagowania na incydenty
- Planowanie awaryjne i kontynuacja działalności
- Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione

6. Aktualne trendy i przyszłość cyberbezpieczeństwa

- Sztuczna inteligencja i machine learning w cyberbezpieczeństwie
- Kryptografia i blockchain
- Bezpieczeństwo danych w erze Big Data
- Przyszłość cyberbezpieczeństwa: wyzwania i możliwości

Przewiduje się, że szkolenie potrwa łącznie minimum 8 godzin roboczych, rozłożonych na co najmniej 2 dni. Każda sesja będzie trwała 4 godziny obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

9. Szkolenie specjalistyczne dla kadry zarządzającej

Zaawansowane Szkolenie z Cyberbezpieczeństwa dla Kadry Zarządzającej

Cel szkolenia:

Przekazanie menedżerom zaawansowanej wiedzy i narzędzi niezbędnych do efektywnej ochrony przed rosnącymi zagrożeniami cybernetycznymi, poprzez pogłębione rozumienie ryzyk, strategii obronnych, regulacji prawnych oraz najnowszych trendów w cyberbezpieczeństwie.

Struktura programu szkoleniowego:

Szkolenie powinno być kompleksowym procesem, który umożliwia uczestnikom zdobycie dogłębnej wiedzy na temat wybranych zagadnień. Powinno ono nie tylko dostarczyć podstawowej informacji, ale także omówić zaawansowane aspekty danej tematyki, aby uczestnicy mieli pełniejsze zrozumienie tematu i byli w stanie zastosować zdobytą wiedzę w praktyce. Przekazywanie wiedzy powinno być interaktywne i angażujące, wykorzystując różnorodne metody nauczania, takie jak prezentacje, dyskusje, studia przypadków czy praktyczne ćwiczenia, co pozwoli uczestnikom efektywniej przyswoić omawiany materiał.

W ramach przeprowadzonego szkolenia wykonawca

1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:

- Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.

- Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskają wgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatak może mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.

2. Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji:

- Normy ISO/IEC: Szczegółowe omówienie serii norm: ISO/IEC 27000: (zarysowuje leksykon oraz globalne zasady nadrzędne systemu zarządzania bezpieczeństwem informacji, kreśląc fundament pod szersze zrozumienie oraz efektywniejsze stosowanie pozostałych norm z rodziny 27000), ISO/IEC 27001 (stanowi kanon dotyczący wymagań dla systemów zarządzania bezpieczeństwem informacji, umożliwiając organizacjom zabezpieczenie informacji pod kątem ich poufności, integralności oraz dostępności przez implementację adekwatnych procedur zarządczych), ISO/IEC 27002 (oferuje referencyjny zbiór praktyk dla organizacji dążących do identyfikacji, wdrażania, utrzymania oraz doskonalenia swoich mechanizmów ochrony informacji w kontekście SZBI), ISO/IEC 27004 (dostarcza metodykę do monitorowania, przeglądu, oceny oraz doskonalenia efektywności systemu zarządzania bezpieczeństwem informacji, akcentując znaczenie mierzalnych wskaźników), ISO/IEC 27005 (zawiera wytyczne dotyczące zarządzania ryzykiem w kontekście bezpieczeństwa informacji, nakreślając proces identyfikacji, oceny oraz zarządzania ryzykiem

informacyjnym), ISO/IEC 27006 (określa wymogi dla organizacji świadczących usługi certyfikacji systemów zarządzania bezpieczeństwem informacji, wyznaczając ramy dla procesu audytu i certyfikacji), ISO/IEC 27013 (podaje wytyczne integrujące system zarządzania bezpieczeństwem informacji z systemem zarządzania usługami IT, promując koherentną i efektywną infrastrukturę zarządzania), ISO/IEC 27017 (koncentruje się na bezpieczeństwie informacji w chmurze, proponując kontrole oraz wytyczne dla dostawców i użytkowników usług przetwarzania w chmurze), ISO/IEC 27018 (ustanawia kodeks praktyk dla ochrony informacji osobowych w chmurze, zgodnie z wymaganiami prywatności i ochrony danych), ISO/IEC 22301 (specyfikuje wymogi dla systemów zarządzania ciągłością działania, umożliwiając organizacjom przygotowanie na incydenty zakłócające normalne funkcjonowanie), ISO/IEC 24762 (zawiera wytyczne dla usług odzyskiwania po awariach w centrach danych i innych środowiskach IT, podkreślając kluczowe elementy potrzebne do przywrócenia operacji IT po katastrofie, ISO/IEC 27036 (skupia się na zarządzaniu bezpieczeństwem informacji w relacjach między organizacjami, oferując wytyczne dotyczące bezpieczeństwa w outsourcingu i partnerstwach biznesowych), ISO/IEC 31000 (dostarcza wytyczne dotyczące zarządzania ryzykiem ogólnym, promując model zarządzania ryzykiem, który można dostosować do różnych typów organizacji i kontekstów), 13501-2 (norma ta przeprowadza proces kategoryzacji reakcji na ogień wyrobów używanych w budownictwie oraz elementów konstrukcyjnych budowli, określając ich parametry odporności na pożary i zachowanie w ekstremalnych warunkach termicznych), norma 1627 (stanowi kryteria odporne na nieautoryzowany dostęp przez systemy zamykające, jak okna, drzwi oraz osłony, hierarchizując je zgodnie z ich zdolnością do stawiania oporu przy próbach sforsowania), norma 12209-04 (wytycza wymagania techniczne oraz procedury badawcze dla mechanizmów blokujących w obszarze budowlanym, takich jak zamki mechaniczne wraz z ich komponentami, oceniając ich funkcjonalność oraz niezawodność.), norma 50131-1 (określa specyfikacje dla systemów alarmowych przeznaczonych do sygnalizacji prób włamania czy napadu, wyznaczając standardy dotyczące ich skuteczności oraz metodyki testowania).

- Omówienie znaczenia powyższych norm i ich w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.

- Inne standardy: Przedstawienie i dyskusja na temat innych standardów:

- ramy dotyczące zarządzania ryzykiem cyberbezpieczeństwa - NIST Cybersecurity Framework;
- ramy dotyczące wdrażania, rozwoju i doskonalenia polityki IT – COBIT;

- zbiór praktyk dotyczący zarządzania usługami IT – ITIL;
- akceptowalna polityka szyfrowania SANS;
- techniki kryptograficzne - ENISA ;
- ramy ochrony informacji i zasobów federalnych agencji rządowych USA - 800-53 rev3.

- Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.

3. Omówienie zaawansowanych strategii ochrony organizacji:

- Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.

- Wprowadzenie do zarządzania incydentami, zdefiniowanie incydentów i wektorów ataku: atak przeprowadzony z nośnika wymiennego lub urządzenia peryferyjnego, atak wykorzystujący metody brute-force w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług, ataki wykonane z poziomu witryny internetowej lub aplikacji internetowej, atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika, naruszenia zasad dopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych kategorii, utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, na przykład laptopa lub urządzenia typu smartfon.

- Szczegółowy opis i kroki zarządzania incydentami:

- wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
- rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;

- analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;

- klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.

- priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje z możliwymi konsekwencjami incydentu dla misji instytucji;

- podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;

- ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.

- Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:

- Priorytet krytyczny - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.

- Priorytet wysoki - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.

- Priorytet średni - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.

- Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.

- Lista omówionych kompetencji w szkoleniu:

- Szef działu bezpieczeństwa (kierownik, dyrektor);
- Pełnomocnik ds. Bezpieczeństwa Informacji;
- Specjalista ds. Zarządzania Ryzykiem;
- Specjalista ds. Zgodności;
- Specjalista ds. Bezpieczeństwa Fizycznego;
- Architekt Systemów Bezpieczeństwa;
- Koordynator Programu Bezpieczeństwa;
- Analityk Bezpieczeństwa (II linia wsparcia);
- Inżynier ds. Bezpieczeństwa (II linia wsparcia);
- Administrator Systemów Bezpieczeństwa (II linia wsparcia);
- Specjalista ds. Odpowiedzi na Incydenty (III linia wsparcia);
- Specjalista ds. Testów Penetracyjnych (III linia wsparcia);
- Specjalista ds. Testów Socjotechnicznych (III linia wsparcia).

4. Regulacje prawne i compliance:

- Zharmonizowanie działalności Podmiotu z imperatywami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, z naciskiem na implementację procedur i protokołów zapewniających wytrzymałość infrastruktury informatycznej na potencjalne zagrożenia cyfrowe.

- Inicjacja, adaptacja, perpetuacja oraz ewolucja Systemu Zarządzania Bezpieczeństwem Informacji, skonstruowanego na fundamencie czterech norm określonych w paragrafie 20 Krajowego Ramienia Interoperacyjności, stanowiących kamień węgielny dla ochrony danych.

- Egzekwowanie procedury tworzenia redundancji danych dziennikowych poprzez generowanie kopii zapasowych, które będą przechowywane przez okres minimalny dwóch lat, zgodnie z dyrektywą zawartą w paragrafie 21 Krajowego Ramienia Interoperacyjności.

- Implementacja kompleksowej agregacji logów (rejestrowanych zdarzeń) pochodzących z heterogenicznej gamy urządzeń, maszyn i aplikacji działających w ramach infrastruktury teleinformatycznej Podmiotu, umożliwiająca szczegółową analizę i audyt bezpieczeństwa.

- Integracja z zaawansowanym systemem zarządzania cyberbezpieczeństwem S46 (S46-react), celem optymalizacji procesów detekcji, reagowania i prewencji w zakresie incydentów bezpieczeństwa cyfrowego.

- Kodyfikacja programu regularnych audytów wewnętrznych i zewnętrznych, obejmujących spektrum standardów i regulacji (KRI, KSC, ISO, RODO), wraz z przeprowadzaniem testów penetracyjnych i socjotechnicznych, mających na celu weryfikację skuteczności implementowanych środków ochrony.

- Monitorowanie zdarzeń systemowych w trybie ciągłym, poprzez wykorzystanie mechanizmów korelacji zdarzeń, umożliwiających identyfikację i interpretację wzorców aktywności sugerujących potencjalne scenariusze ataków cybernetycznych.

- Dostosowanie się do rozszerzonego zakresu wymagań wynikających z implementacji Dyrektywy NIS2, która wprowadza nowe, zaostrzone standardy w zakresie cyberbezpieczeństwa, wymagające od organizacji ponownej oceny i ulepszenia istniejących strategii ochrony danych.

- Wyznaczenie dedykowanego Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, którego rola nie będzie interferować ani generować konfliktów interesów z innymi kluczowymi funkcjami w organizacji (np. Inspektorem Ochrony Danych, Informatykiem, Dyrektorem).

- Rekonfiguracja systemów informatycznych oraz protokołów pracy zdalnej w zgodzie ze zmienionymi standardami bezpieczeństwa, uwzględniającymi nowelizację Kodeksu Pracy, w celu zabezpieczenia integralności danych korporacyjnych w rozproszonym środowisku pracy.

- Realizacja oczekiwań organów nadzorczych w kontekście konstruowania oraz utrzymywania zaawansowanych systemów cyberbezpieczeństwa, zdolnych do przeciwdziałania współczesnym zagrożeniom w przestrzeni cyfrowej.

- Implementacja rygorystycznych protokołów ochrony danych osobowych, mających na celu eliminację ryzyka wycieków informacji, spowodowanych przez nieświadome bądź intencjonalne działania personelu organizacji.

- Automatyzacja procesów aktualizacji oprogramowania w celu zapewnienia najwyższego poziom

5. Zarządzanie bezpieczeństwem w praktyce:

- Zrozumienie znaczenia typów licencji względem konieczności ich testowania:

- Licencje niewyłączne, w których udzielający licencji może zezwolić na korzystanie z utworu wielu osobom równocześnie, które nie muszą mieć formy pisemnej.

- Licencje wyłączne, spotykane głównie w przypadku oprogramowania pisanego na zamówienie (np. strona www), w tym przypadku zwykle umowa licencyjna wynika z umowy o dzieło, na podstawie której firma wykonująca oprogramowanie wykonuje zamówioną aplikację, umowa taka wymaga formy pisemnej pod rygorem nieważności.

- Sublicencja, w której licencjobiorca może udzielić dalszej licencji, pod warunkiem wszakże takiego upoważnienia w jego umowie licencyjnej.

- OEM, to programy sprzedawane wraz ze sprzętem komputerowym (przypisane do konkretnego komputera), po wymianie sprzętu na nowszy, nie można ich przenieść na nowy komputer tylko trzeba ponownie je zakupić.

- BOX, to programy, które można przenosić na kolejne komputery jednak pod warunkiem, że zawsze zainstalowany jest tylko na jednym komputerze. Legalny jest tylko program ostatnio zainstalowany.

- Open Source (otwarte oprogramowanie) to alternatywa dla Freeware (wolne oprogramowanie), którego celem jest istnienie swobodnego dostępu do oprogramowania dla wszystkich jego uczestników. Zapewnia swoim użytkownikom prawo do legalnego oraz darmowe.

- Techniki hardeningu: Wzmocnienie infrastruktury IT oraz zarządzanie patchami bezpieczeństwa.

- Testy penetracyjne i socjotechniczne: Organizacja i przeprowadzanie testów w celu oceny gotowości organizacji

Szkolenie powinno odbyć się w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem conajmniej 4 przerw po 15 minut. Po szkoleniu przewidziano 30 minut na pytania i odpowiedzi uczestników.

10. Szkolenie specjalistyczne dla informatyków

Szkolenie z obsługi oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej Przedmiotem zamówienia jest przeprowadzenie szkolenia stacjonarnego lub online dla personelu IT, w celu przekazania kompletnej wiedzy w zakresie obsługi i wykorzystania funkcji oprogramowania zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej w ich codziennej pracy.
Szkolenie obejmie co najmniej następujące obszary:
A. Wprowadzenie do oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych: Omówienie podstawowych koncepcji związanych z oprogramowaniem do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, takich jak zarządzanie urządzeniami, oprogramowaniem i konfiguracjami.
B. Interfejs użytkownika: Przewodnik po interfejsie użytkownika oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, pokazujący główne funkcje i narzędzia dostępne dla administratorów.

C. Zarządzanie urządzeniami: Szkolenie w zakresie dodawania, konfigurowania i monitorowania urządzeń oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, w tym zarządzanie grupami i politykami.
D. Zarządzanie oprogramowaniem: Instrukcje dotyczące instalowania, aktualizowania i monitorowania oprogramowania na urządzeniach za pomocą oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych.
E. Automatyzacja procesów: Szkolenie związane z automatyzacją rutynowych zadań administracyjnych za pomocą skryptów i zadań zaplanowanych dla oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych.
F. Bezpieczeństwo: Omówienie funkcji związanych z zabezpieczeniami oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, takich jak zarządzanie aktualizacjami, ochrona przed złośliwym oprogramowaniem i polityki bezpieczeństwa.
G. Wsparcie użytkowników końcowych: Instrukcje dotyczące udzielania pomocy technicznej użytkownikom końcowym oraz rozwiązywania problemów związanych z urządzeniami i oprogramowaniem.
H. Raportowanie i analiza: Szkolenie z generowania raportów i analizy danych dla oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych w celu monitorowania wydajności i zgodności z wymaganiami.
I. Scenariusze praktyczne: Przeprowadzenie praktycznych ćwiczeń i scenariuszy, aby umożliwić uczestnikom praktyczne zastosowanie wiedzy zdobytej podczas szkolenia.
J. Ewaluacja: Przeprowadzenie ewaluacji, aby ocenić skuteczność szkolenia i zidentyfikować obszary do dalszego doskonalenia.
Czas trwania szkolenia przewidziano na co najmniej 2 dni robocze z uwzględnieniem przerw 3 przerw po 15 minut. Po szkoleniu Wykonawca udostępni co najmniej 4 godziny robocze na dodatkowe pytania i odpowiedzi uczestników przez okres 30 dni.

11. Szkolenie specjalistyczne dla informatyków

Szkolenie z obsługi oprogramowania przeciwdziałającego wyciekowi danych

Przedmiotem zamówienia jest przeprowadzenie szkolenia stacjonarnego lub online dla personelu IT, w celu przekazania kompletnej wiedzy w zakresie obsługi i wykorzystania funkcji oprogramowania przeciwdziałającego wyciekowi danych, w ich codziennej pracy.

Szkolenie obejmie co najmniej następujące obszary:

- Podstawowe informacje
- Licencjonowanie
- Wspierane systemy operacyjne

- Wdrożenie oprogramowania przeciwdziałającego wyciekowi danych
- Omówienie instalatora oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie serwera oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie agentów oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie klientów oprogramowania przeciwdziałającego wyciekowi danych
- Uruchomienie modułu analitycznego
- Analiza wycieków danych
- Filtrowanie i raporty z analizy
- Uruchomienie modułu przeciwdziałającego wyciekowi danych
- Uruchomienie szyfrowania BitLockerem
- Konfiguracja dostępu do urządzeń i portów
- Interfejs webowy oprogramowania przeciwdziałającego wyciekowi danych
- Minimalne wymagania systemowe dla omawianego oprogramowania
- Instalacja oraz konfiguracja modułu webowego oprogramowania przeciwdziałającego wyciekowi danych
- Analiza zachowań
- Zarządzenie kategoriami produktywności
- Kontrola WWW i aplikacji

- Alerty, raporty i konserwacja
- Zaawansowane DLP dla oprogramowania przeciwdziałającego wyciekowi danych
- Reguły DLP – tryby polityk
- Reguły ogólne
- Reguły aplikacji
- Po co nam kategorie danych?
- Inteligentne wyszukiwanie danych osobowych
- Czym są tagi i do czego służą?
- Reguły tagowania dla aplikacji, stron oraz lokalizacji

12. Szkolenie specjalistyczne dla informatyków

Przedmiotem zamówienia jest przeprowadzenie kompleksowego szkolenia z zakresu obsługi i zarządzania systemem Security Information and Event Management (SIEM). Celem szkolenia jest zapewnienie uczestnikom wiedzy i umiejętności niezbędnych do efektywnego monitorowania, wykrywania oraz reagowania na zagrożenia bezpieczeństwa w czasie rzeczywistym.

Szkolenie będzie obejmować następujące zagadnienia:

1. Wprowadzenie do systemów SIEM oraz ich roli w zapewnianiu bezpieczeństwa informacji.

2. Omówienie możliwości systemów SIEM, w tym analiza logów, wykrywanie intruzów, reagowanie na zagrożenia oraz integracja z innymi narzędziami bezpieczeństwa.

3. Praktyczne aspekty zbierania, agregowania, indeksowania i analizowania danych bezpieczeństwa, w celu identyfikacji włamań, zagrożeń oraz anomalii behawioralnych.

4. Zarządzanie podatnościami: metody identyfikacji słabości systemów i aplikacji, oraz techniki korelowania ich z aktualnymi bazami danych dotyczącymi podatności.

5. Ocena konfiguracji systemu i aplikacji zgodnie z najlepszymi praktykami i standardami, w tym analiza zgodności z regulacjami takimi jak RODO/GDPR, PCI DSS, NIST.

6. Reagowanie na incydenty: strategie i procedury tworzenia reguł alarmowych oraz zarządzanie reakcją na wykryte zagrożenia.

7. Przykłady zastosowania i najlepsze praktyki w wykorzystaniu systemów SIEM w różnych środowiskach, w tym w infrastrukturze chmurowej i w systemach kontenerowych.

Szkolenie ma na celu przygotowanie uczestników do samodzielnego zarządzania systemem SIEM, zrozumienia zasad ich działania oraz umiejętności konfiguracji i adaptacji systemu do specyficznych potrzeb organizacji. Uczestnicy nauczą się, jak efektywnie monitorować i analizować bezpieczeństwo w swoich systemach, identyfikować i reagować na zagrożenia, a także jak stosować najlepsze praktyki w celu zwiększenia ogólnego poziomu bezpieczeństwa informacji.

Czas trwania szkolenia przewidziano na 8 godzin roboczych w ciągu jednego dnia, z uwzględnieniem 4 przerw po 15 minut. Po dniu szkolenia będzie 30 minut na pytania i odpowiedzi uczestników.

Przedmiotem zamówienia jest przeprowadzenie kompleksowego szkolenia z zakresu obsługi i zarządzania systemem monitorowania infrastruktury IT. Celem szkolenia jest zapewnienie uczestnikom wiedzy i umiejętności niezbędnych do efektywnego monitorowania infrastruktury IT, wykrywania problemów oraz reagowania na nie w czasie rzeczywistym.

Zagadnienia szkolenia:

1. Wprowadzenie do systemu monitorowania:
   - Podstawowe informacje o systemach monitorowania.
   - Rola monitorowania w zapewnianiu ciągłości działania i bezpieczeństwa systemów IT.
2. Architektura systemu monitorowania:
   - Omówienie komponentów systemu monitorowania.

- Instalacja i konfiguracja serwera monitorowania, agenta oraz interfejsu webowego.

3. **Konfiguracja monitorowania**:

- Tworzenie i zarządzanie hostami i szablonami.
- Konfiguracja elementów monitorowania (items) oraz wyzwalaczy (triggers).

4. **Zbieranie i analiza danych**:

- Metody zbierania danych (agent, SNMP, IPMI, JMX, etc.).
- Praktyczne aspekty agregowania i analizowania danych monitorowania.

5. **Zarządzanie zdarzeniami i alarmami**:

- Definiowanie akcji oraz eskalacji alarmów.
- Integracja z systemami powiadomień (e-mail, SMS, webhooki).

6. **Wizualizacja danych**:

- Tworzenie i zarządzanie dashboardami.
- Generowanie raportów i wizualizacji danych.

7. **Najlepsze praktyki i studia przypadków**:

- Przykłady zastosowania systemu monitorowania w różnych środowiskach (on-premises, chmurowe, kontenerowe).
- Najlepsze praktyki w monitorowaniu bezpieczeństwa i wydajności.

8. **Zaawansowane funkcje systemu monitorowania**:

- Korzystanie z LLD (Low-Level Discovery).
- Monitorowanie wydajności aplikacji (APM).
- Automatyzacja zadań z wykorzystaniem skryptów i API systemu monitorowania.

Cel szkolenia:

Szkolenie ma na celu przygotowanie uczestników do samodzielnego zarządzania systemem monitorowania, zrozumienia zasad jego działania oraz umiejętności konfiguracji i adaptacji systemu do specyficznych potrzeb organizacji. Uczestnicy nauczą się, jak efektywnie monitorować i analizować infrastrukturę IT, identyfikować i reagować na problemy oraz jak stosować najlepsze praktyki w celu zwiększenia ogólnego poziomu wydajności i bezpieczeństwa.

Harmonogram szkolenia:

Czas trwania szkolenia przewidziano na 8 godzin roboczych w ciągu jednego dnia, z uwzględnieniem 4 przerw po 15 minut. Po dniu szkolenia będzie 30 minut na pytania i odpowiedzi uczestników.

13. Wdrożenie systemów teleinformatycznych

Usługi wdrożeniowe oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej.

A. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.

B. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.

C. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.

D. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.

E. Wykonawca zainstaluje oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej, na wskazanym serwerze lokalnym lub w chmurze i skonfiguruje je zgodnie z wymaganiami i najlepszymi praktykami.

F. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.

G. Wykonawca przeprowadzi konfigurację strefy DMZ dla wymaganych usług.

H. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.

I. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze.

J. Wykonawca przeprowadzi testy zarządzania urządzeniami, w tym możliwość dodawania, usuwania i zarządzania urządzeniami w konsoli administracyjnej oprogramowania oraz poprawność

wykonywania instalacji, aktualizacji i usuwania oprogramowania. Wykonawca przetestuje, że konfiguracje mogą być efektywnie stosowane na wybranych urządzeniach.

K. Wykonawca przeprowadzi testy zdalnego zarządzania poprzez zdalne sterowanie komputerem oraz zdalne wsparcie ekranowe. Wykonawca w ramach tego zadania zweryfikuje dodatkowo czy można efektywnie udzielać pomocy technicznej użytkownikom poprzez konsolę oprogramowania.

L. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje na temat stanu infrastruktury IT oraz czy możliwość monitorowania wydajności urządzeń i systemów za pomocą narzędzi dostępnych w oprogramowaniu działa prawidłowo, zgodnie z założeniami prawidłowego działania oprogramowania.

M. Wykonawca przeprowadzi testy zabezpieczeń, weryfikując czy zastosowane zabezpieczenia, takie jak zasady bezpieczeństwa i ochrona antywirusowa, są skutecznie wdrażane na urządzeniach.

N. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.

O. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii

14. Wdrożenie systemów teleinformatycznych

Dostawa i wdrożenie oprogramowania do monitorowania zasobów IT:

Wymagania w zakresie oprogramowania:

- Automatyczne odkrywanie sieci.

- Monitorowanie wydajności i dostępności.
- Zaawansowane wizualizacje danych, w tym wykresy, mapy i wykresy słupkowe.
- Wbudowane narzędzia do przetwarzania i analizy danych.
- Możliwość monitorowania przez SNMP, JMX, IPMI, agenta Zabbix i inne.
- Szeroka gama integracji z zewnętrznymi systemami.
- Elastyczność w konfiguracji elementów monitorowanych.
- Wsparcie dla monitorowania aplikacji, serwerów, sieci i urządzeń.
- Możliwość definiowania scenariuszy monitorowania.
- Rozbudowane opcje powiadomień i alarmów.
- Wsparcie dla skryptów i automatyzacji zadań.
- Monitorowanie transakcji biznesowych i aplikacji webowych.
- Wbudowane rozwiązania do diagnostyki i rozwiązywania problemów.
- Możliwość tworzenia niestandardowych wskaźników monitorowania.
- Skalowalność i możliwość monitorowania tysięcy urządzeń.
- Wsparcie dla monitorowania w chmurze i środowiskach wirtualnych.
- Zaawansowane raportowanie i analizy trendów.
- Integracja z systemami ticketowymi.
- Możliwość tworzenia dashboardów i paneli.

- Wsparcie dla różnorodnych systemów operacyjnych.
- Elastyczne opcje autentykacji i kontroli dostępu.
- Szyfrowanie komunikacji.
- Możliwość monitorowania baz danych.
- Wsparcie dla wysokiej dostępności i redundancji.
- Automatyczne odkrywanie urządzeń w sieci.
- Monitorowanie wykorzystania zasobów.
- Możliwość śledzenia zmian konfiguracyjnych.
- Integracja z rozwiązaniami do zarządzania konfiguracją.
- Możliwość zbierania danych z różnych źródeł.
- Wsparcie dla monitorowania środowisk kontenerowych.
- Możliwość definiowania zależności między monitorowanymi elementami.
- Zaawansowane filtrowanie i wyszukiwanie danych.
- Możliwość monitorowania poprzez proxy.
- Wsparcie dla niestandardowych skryptów monitorujących.
- Automatyczne wykrywanie problemów i anomalii.
- Możliwość grupowania urządzeń i aplikacji.
- Wsparcie dla monitorowania sieciowych urządzeń peryferyjnych.

- Możliwość tworzenia template'ów monitorowania.
- Wsparcie dla różnych metod zbierania danych (polling, trapper, SNMP traps).
- Możliwość tworzenia hierarchii monitorowania.
- Wsparcie dla wielojęzyczności interfejsu użytkownika.
- Możliwość zarządzania poprzez interfejs webowy.
- Zaawansowane opcje logowania i audytu.
- Wsparcie dla monitorowania poprzez protokół HTTPS.
- Możliwość definiowania zdarzeń i akcji.
- Możliwość monitorowania szyfrowanych połączeń.
- Integracja z systemami zarządzania logami.
- Wsparcie dla SNMP v3.
- Możliwość definiowania i monitorowania SLA.
- Wsparcie dla rozproszonego monitoringu.

Wymagania w zakresie wdrożenia oprogramowania:

Krok 1: Planowanie i Przygotowanie

- Określenie wymagań dotyczących monitorowania, obejmujące zarówno liczbę urządzeń, które będą monitorowane, jak i typy parametrów, których monitorowanie jest kluczowe dla działania infrastruktury IT. Dodatkowo, konieczne jest sprecyzowanie oczekiwanych powiadomień w przypadku wykrycia nieprawidłowości lub awarii.

- Dokonanie wyboru odpowiedniej platformy do instalacji narzędzia monitorującego, uwzględniając różnice między systemem operacyjnym Linux a Windows. W tym procesie istotne jest także przypisanie odpowiednich zasobów sprzętowych i sieciowych, aby zapewnić odpowiednią wydajność i dostępność narzędzia.

- Pobranie najnowszej wersji wybranego narzędzia do monitorowania zasobów IT oraz dokładnie zapoznaj się z dokumentacją. Zapoznanie się z dokumentacją pozwoli na lepsze zrozumienie funkcjonalności narzędzia oraz prawidłową konfigurację i wykorzystanie jego możliwości w procesie monitorowania infrastruktury IT.

Krok 2: Instalacja i Konfiguracja serwera (procesu centralnego) narzędzia do monitorowania zasobów IT

- Przeprowadzenie instalacji serwera, który pełni rolę centralnego procesu narzędzia do monitorowania zasobów IT. Począwszy od wybranej platformy, postępujemy zgodnie z precyzyjnie określonymi instrukcjami instalacyjnymi, które są dostępne w dokumentacji danego rozwiązania.

- Konfiguracja centralnego procesu narzędzia. W ramach konfiguracji, należy zapewnić odpowiedni dostęp do bazy danych. Możesz użyć różne systemy zarządzania bazami danych, takie jak MySQL, PostgreSQL lub SQLite.

- Ustalenie parametrów monitorowania, które obejmują specyficzne aspekty środowiska IT podlegające monitorowaniu. Dodatkowo, konieczne jest skonfigurowanie powiadomień, aby zapewnić odpowiednie reakcje na wykryte nieprawidłowości czy awarie. Poprzez precyzyjne skonfigurowanie tych ustawień, można efektywnie zarządzać monitorowanymi zasobami IT oraz szybko reagować na wszelkie pojawiające się problemy.

Krok 3: Instalacja i Konfiguracja Agentów wybranego narzędzia na Monitorowanych Hostach

- Instalacja agentów na wszystkich urządzeniach, które podlegają monitorowaniu, obejmując serwery, routery, przełączniki oraz inne istotne elementy infrastruktury IT.

- Konfiguracja agentów, aby komunikowały się z wcześniej zainstalowanym i skonfigurowanym serwerem.

- Określenie parametrów komunikacji, takich jak adres serwera monitorującego oraz porty, aby umożliwić płynną wymianę danych pomiędzy agentami a serwerem.

Krok 4: Konfiguracja Monitorowanych Parametrów i Wykresów

- Konfiguracja elementów monitorowania, takich jak elementy, wykresy, triggery i akcje, aby monitorować ważne parametry systemowe i aplikacyjne. Umożliwi to kompleksowe śledzenie wybranych parametrów, takich jak obciążenie CPU, zużycie pamięci, dostępność usług, wydajność aplikacji.

- Dostosowanie progów alarmowych dla trigerów, w celu uzyskania optymalnych powiadomień o ewentualnych awariach lub nieprawidłowościach w działaniu systemu. Warto zadbać o precyzyjne ustalenie progów alarmowych, aby uniknąć fałszywych alarmów oraz zapewnić skuteczną ochronę środowiska IT.

Krok 5: Testowanie i Optymalizacja

- Weryfikacja skonfigurowanych monitorów i triggerów, aby upewnić się, że działają zgodnie z oczekiwaniami. Testowanie powinno obejmować różne scenariusze działania systemu, aby zweryfikować skuteczność monitorowania w różnych warunkach. Poprawne działanie monitorów i trigerów jest kluczowe dla zapewnienia szybkiej reakcji na ewentualne problemy.

- Optymalizacja konfiguracji narzędzia do monitorowania zasobów IT, w celu zapewnienia wydajności i skuteczności monitorowania, np. poprzez dostosowanie interwałów sprawdzania.

Krok 6: Monitorowanie i Administracja

- Regularne monitorowanie stanu urządzeń i aplikacji za pomocą interfejsu narzędzia do monitorowania zasobów IT pozwoli szybko identyfikować ewentualne zagrożenia lub nieprawidłowości w działaniu systemu, co umożliwia szybką reakcję i zapobieganie poważnym problemom.

- Reagowanie na alarmy i zdarzenia, które występują w środowisku monitorowanym.
  W przypadku pojawiających się alarmów i zdarzeń, podejmować niezbędne działania naprawcze w celu przywrócenia normalnego funkcjonowania systemu.

- Regularne aktualizowanie oprogramowania do monitorowania zasobów IT, zapewni dostęp do najnowszych funkcji i poprawek bezpieczeństwa, co jest kluczowe dla utrzymania wysokiej jakości monitorowania oraz zapewnienia zgodności z aktualnymi standardami i wymaganiami branżowymi.

15. Wdrożenie systemów teleinformatycznych

Dostawa oraz wdrożenie oprogramowania typu SIEM

Zamawiający na potrzeby instalacji i wdrożenia udostępni infrastrukturę na serwerach zwirtualizowanych, wg. specyfikacji uzgodnionych z Wykonawcą. Czynności związane z wdrożeniem systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja systemu przez Wykonawcę odbywać się będzie z wykorzystaniem środków komunikacji elektronicznej.

Wykonawca zobowiązuje się do dostarczenia kompleksowego oprogramowania typu Security Information and Event Management (SIEM), które będzie spełniało poniższe wymagania funkcjonalne i techniczne.

Funkcjonalności systemu.

- Monitorowanie występujących zdarzeń (logów) w trybie ciągłym.

- Zbieranie zdarzeń z serwerów wirtualnych, fizycznych, Active Directory, przełączników oraz innego rodzaju urządzeń, które są oraz zostaną podłączone do infrastruktury zamawiającego.

- Agregacja oraz korelacja logów.

- Wykrywanie ataków typu brute force na różne usługi.

- Wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu.
- Analiza logów w oparciu o wbudowane reguły bezpieczeństwa.
- Konfiguracja oprogramowania do przechowywania logów z kluczowych zasobów przez okres 24 miesięcy zgodnie z rozporządzeniem KRI §21 pkt. 4 „Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.”
- Panel do wyszukiwania zdarzeń.

Wdrożenie systemu.

Wykonawca będzie odpowiedzialny za instalację i konfigurację oraz optymalizację środowiska systemu w infrastrukturze Zamawiającego oraz opiekę serwisową i wsparcie techniczne przez okres 30 dni.

Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:

- Przedstawienie architektury systemu.
- Omówienie procedur obsługi administracyjnej systemu;
- Omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń systemu;
- Przekazanie informacji na temat konfiguracji i zarządzania systemem;
- Instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną.

16. Wdrożenie systemów teleinformatycznych

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

A. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.

B. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.

C. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.

D. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.

E. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.

F. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.

G. Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.

H. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.

I. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.

J. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

- Numery kart kredytowych
- Numery IBAN
- Numery dowodów osobistych
- Polski numer paszportu
- Numer PESEL

K. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.

L. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.

M. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.

N. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.

O. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.

P. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.

Q. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

V Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV)

Główny kod CPV:
72263000-6 - Usługi wdrażania oprogramowania
Dodatkowy kod CPV:
80511000-9 - Usługi szkolenia personelu
80510000-2 - Usługi szkolenia specjalistycznego
72220000-3 - Usługi doradcze w zakresie systemów i doradztwo techniczne

VI Miejsce i Terminy wykonania zamówienia

Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Wdrożenia będą realizowane w ciągu 120 dni, szkolenia w ciągu 180 dni.

Przedmiot umowy będzie dostarczany przez Wykonawcę do miejsc wskazanych przez Zamawiającego w zakresie dostawy sprzętu/oprogramowania/licencji.

Zamawiający może zawrzeć umowę w sprawie przedmiotowego zamówienia publicznego przed upływem terminu, jeżeli w przedmiotowym postępowaniu zostanie złożona tylko jedna oferta.

VII Warunki udziału w postępowaniu

1. udzielenie zamówienia mogą się ubiegać wykonawcy, którzy:
   - nie podlegają wykluczeniu na podstawie ustawy prawo zamówień publicznych,

- spełniają warunki udziału w postępowaniu w zakresie kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile obowiązek ich posiadania wynika z odrębnych przepisów. Zamawiający nie określa szczegółowo ww. warunku.
- spełniają warunki udziału w postępowaniu w zakresie sytuacji ekonomicznej lub finansowej. Zamawiający nie określa szczegółowo ww. warunku.
- spełniają warunki udziału w postępowaniu w zakresie zdolności technicznej lub zawodowej.

2. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Na potwierdzenie spełnienia warunku udziału w postępowaniu, dotyczącego zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca wykazał się odpowiednim doświadczeniem, tj. w ciągu ostatnich 3 lat przed upływem terminu składania ofert, w tym okresie realizuje, bądź zrealizował należycie co najmniej dwie usługi w zakresie dostawy oprogramowania komputerowego na kwotę co namniej 150 000 złotych brutto.
4. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
5. Wykonawca, który polega na zdolnościach innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

VIII Przesłanki wykluczenia Wykonawcy

1. Zamawiający wykluczy wykonawcę z postępowania o udzielenie zamówienia, w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych w art. 108 ust. 1 ustawy Pzp, tj.:

1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz.U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust.1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz.U. z 2021 r. poz. 523, 1292, 1559 i 2054),
d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),
g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej - lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego; 2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo

komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

2. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
3. jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie.
4. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.
5. Zamawiający nie wprowadza w tym postępowaniu dodatkowych podstaw wykluczenia wskazanych w art. 109 ustawy Pzp.
6. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy Pzp.
7. Jeżeli wykonawca polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby zamawiający zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.
8. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia zgodnie z art. 110 ust. 1 ustawy Pzp.
9. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt. 1, 2 i 5 ustawy Pzp, jeśli udowodni zamawiającemu, że spełnił przesłanki wskazane w art. 110 ust. 2 ustawy Pzp. Zamawiający oceni, czy podjęte przez wykonawcę czynności o których mowa w art. 110 ust. 2 ustawy Pzp są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności, o których mowa w art. 110 ust. 2 ustawy Pzp, nie są wystarczające do wykazania rzetelności, zamawiający wykluczy wykonawcę.
10. Ponadto Zamawiający wykluczy z postępowania o udzielenie zamówienia Wykonawcę, w stosunku, do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 7 ust. 1 zgodnie z ustawą o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z dnia 13 kwietnia 2022 roku (Dz. U. z 2022, poz. 835).

VIX Obowiązek zatrudniania przez wykonawcę osób na podstawie stosunku pracy (art. 95 PZP)

1. Zamawiający wymaga aby osoby odpowiedzialne za koordynację wykonania zamówienia po Stronie Wykonawcy (pracownik administracyjny/biurowy/stanowisko równoważne) zatrudniona była na podstawie stosunku pracy, o którym mowa w art. 22 § 1 Kodeksu pracy.
2. Obowiązek określony powyżej dotyczy również podwykonawców
3. W celu weryfikacji zatrudniania, przez wykonawcę lub podwykonawcę, na podstawie umowy o pracę, osób wykonujących wskazane przez zamawiającego czynności w zakresie realizacji zamówienia, Zamawiający wymaga złożenia oświadczenia wykonawcy lub podwykonawcy o zatrudnieniu pracownika na podstawie umowy o pracę.

4. Pozostałe osoby uczestniczące w wykonaniu zamówienia mogą współpracować z Wykonawcą na podstawie umów cywilnoprawnych.
5. W przypadku uzasadnionych wątpliwości co do przestrzegania prawa pracy przez Wykonawcę lub Podwykonawcę, Zamawiający może zwrócić się o przeprowadzenie kontroli przez Państwową Inspekcję Pracy.

X Wykaz oświadczeń lub dokumentów, jakie mają złożyć wykonawcy w celu wykazania spełniania warunków udziału w postępowaniu oraz niepodlegania wykluczeniu z postępowania

1. Wykaz podmiotowych środków dowodowych: 3.1. Zgodnie z art. 274 ust. 1 ustawy Pzp, zamawiający przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia, następujących podmiotowych środków dowodowych:

- Wykaz dostaw wykonanych w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - tj.w tym okresie, wraz z podaniem ich wartości, dat wykonania i podmiotów na rzecz, których usługi zostały wykonane, przed upływem terminu składania ofert, w co najmniej dwóch usług w zakresie dostawy oprogramowania komputerowego na kwotę co najmniej 150 000 złotych brutto wraz z dowodem należytego ich wykonania.
- Aktualne na dzień składania ofert oświadczenia, stanowiące wstępne potwierdzenie, że nie podlega wykluczeniu z postępowania,
- Aktualne na dzień składania ofert oświadczenie sankcyjne,
- Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu, zamieszcza informacje o tych podmiotach w oświadczeniach,

2. Zamawiający wymaga od Wykonawcy złożenia wraz z ofertą następujących przedmiotowych środków dowodowych w celu potwierdzenia zgodności oferowanych produktów z wymaganiami Zamawiającego w zakresie wskazanym w zestawieniu poniżej:
   - co najmniej dwa z trzech certyfikatów: MS 50255 Managing, Maintaining, and Securing Your Networks Through Group Policy, SC-900 Microsoft Certified: Security, Compliance, and Identity Fundamentals, MS-55341 Installation, Storage, and Compute with Windows Server, w zakresie usług i rozwiązań opartych o środowisko Microsoft;
   - ITIL® Foundation Certificate in IT Service Management w zakresie projektowania, zrozumienia i zastosowania najlepszych praktyk w zarządzaniu usługami informatycznymi;
   - co najmniej dwa z trzech certyfikatów: Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE), Certified Professional Penetration Tester (eCPPTv2) w zakresie testowania I weryfikacji poprawności wdrażanych rozwiązań,

3. W odniesieniu do pozostałych przedmiotowych środków dowodowych zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane dostawy spełniają określone przez zamawiającego wymagania, cechy i kryteria.

4. Zamawiający informuje, że działając na podstawie art. 107 ust. 2 ustawy Pzp przewiduje, że w sytuacji, w której Wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, Zamawiający jednokrotnie wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.

Postanowień pkt 4 SWZ nie stosuje się:

a) w części w jakiej przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub,

b) pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.

Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści przedmiotowych środków dowodowych.

5. Wykonawca jest zobowiązany do wypełnienia obowiązku informacyjnego przewidzianego w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał (w przypadku korzystania z podwykonawców/ podmiotów trzecich/wykonawców wchodzących w skład konsorcjum) w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

XI Poleganie na zasobach podmiotów trzecich

1. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z wnioskiem o dopuszczenie do udziału w postępowaniu albo odpowiednio wraz z ofertą, zobowiązanie podmiotu trzeciego do oddania do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
2. Zobowiązanie podmiotu udostępniającego zasoby potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   - zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
   - sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   - czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje dostawy lub usługi, których wskazane zdolności dotyczą.
3. Podwykonawcy obowiązani są do złożenia wszelkich oświadczeń, w szczególności oświadczeń sankcyjnych i o braku przesłanek wykluczenia w takim zakresie w jakim dotyczą one Wykonawcy.

XII Podwykonawstwo

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).
2. Zamawiający **nie zastrzega** obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.

XIII Informacja dla wykonawców polegających na zasobach innych podmiotów, na zasadach określonych w art. 118 ustawy PZP

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
4. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
5. Zobowiązanie podmiotu udostępniającego zasoby lub inny środek dowodowy, o którym mowa w pkt 9.4 SWZ potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
6. 1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
7. 2) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
8. 3) czy i w jakim zakresie podmiot udostępniający zasoby, 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.

9. Zamawiający oceni, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu a także zbada, czy nie zachodzą, wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
10. Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą, wobec tego podmiotu podstawy wykluczenia, Zamawiający zażąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
11. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia oświadczenia podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.

XIV Kryterium równoważności

1. Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych rozwiązaniom wskazanym przez Zamawiającego. Wykonawca oferując rozwiązanie równoważne do opisanego powyżej jest zobowiązany wykazać (udowodnić) równoważność w zakresie wskazanych parametrów, które muszą być na poziomie nie gorszym niż parametry wskazane przez Zamawiającego - Wykonawca musi wykazać (udowodnić), iż proponowane rozwiązanie w równoważnym stopniu spełnia wymagania określone w zapytaniu ofertowym, w szczególności w zakresie parametrów. Jeżeli w opisie przedmiotu zamówienia znajdują się jakiekolwiek odniesienia do określonego wyrobu, źródła, znaków towarowych, patentów czy pochodzenia lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę – należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza składanie ofert równoważnych, w szczególności o parametrach technicznych, użytkowych, funkcjonalnych i jakościowych nie gorszych niż te, podane w opisie przedmiotu zamówienia.

XV Opis sposobu składania ofert w postępowaniu

1. Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej.
2. Preferuje się , aby komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane były za pośrednictwem https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl Zamawiający informuje, że instrukcje korzystania z platformy dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu znajdują się w zakładce „Pomoc" na stronie internetowej pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/pomoc
3. Ofertę wraz z oświadczeniami i dokumentami należy złożyć w terminie do dnia 22-04-2025 r. za pośrednictwem https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl
4. Oferta powinna zawierać:
   Formularz oferty;

- Pełnomocnictwo do reprezentowania Wykonawcy, w tym podpisania oferty, o ile prawo do podpisania oferty nie wynika z innych dokumentów złożonych wraz z ofertą. Treść pełnomocnictwa musi jednoznacznie określać czynności, co do wykonywania których pełnomocnik jest upoważniony;
- Wyjaśnienia uzasadniające zastrzeżenie tajemnicy przedsiębiorstwa (jeżeli dotyczy);
- Oświadczenia i dokumenty o których mowa w treści niniejszej SWZ.

5. Otwarcie ofert nastąpi 23-04-2025 r.
6. Wykonawca nie może wprowadzić zmian do złożonej oferty.
7. Wykonawca może przed upływem terminu składania ofert wycofać ofertę.

XVI Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	70
2.	Doświadczenie z zakresu szkoleń	15
3.	Przyjmowanie możliwości wykonania zamówienia poza godzinami 7.30-15.30 tj. przez całą dobę	15

a. Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.

b. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.

c. Przy ocenie ofert w kryterium „Cena” (C) punkty zostaną przyznane w poniższy sposób:

- Cena – znaczenie 70% (maksymalnie do 70 pkt)
- Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
- Punkty w kryterium „Cena” będą obliczane na podstawie wzoru:
  C = CC min/ CC of x 70

  gdzie:

  C – punkty przyznane Wykonawcy w ramach kryterium „Cena”

  CC min – najniższa cena brutto spośród badanych ofert

  CC of – cena brutto badanej ofert

- Do wzoru zostaną przyjęte ceny podane przez Wykonawców w Formularzu Oferty stanowiącym Załącznik nr 1 do SWZ.

d. Kryterium „Doświadczenie z zakresu szkoleń z cyberbezpieczeństwa”: suma zadeklarowanych przez Wykonawcę wykonanych szkoleń z cyberbezpieczeństwa w okresie 3 ostatnich lat, a jeżeli okres prowadzenia działalności jest krótszy — w tym okresie - 15 pkt.

Zamawiający przyzna punkty w niniejszym kryterium zgodnie z następującymi zasadami:

Liczba przeprowadzonych szkoleń z cyberbezpieczeństwa

- od 1 do 5 przeprowadzonych szkoleń – 5 pkt
- od 6 do 10 przeprowadzonych szkoleń - 10 pkt
- do 11 do 15 przeprowadzonych szkoleń - 15 pkt

Punkty za kryterium doświadczenie będą przyznawane na podstawie liczby wykonanych szkoleń zadeklarowanych przez Wykonawcę w Formularzu Ofertowym stanowiący integralną część oferty.

e. Kryterium „Przyjmowanie możliwości wykonania zamówienia poza godzinami 7.30-15.30 tj. przez całą dobę” stanowi 15 możliwych do uzyskania punktów.

f. Sumaryczna liczba punktów zostanie obliczona według wzoru:

W = C + D + E

gdzie:

W – łączna liczba punktów przyznanych w poszczególnych kryteriach,

C – liczba punktów przyznanych w kryterium „Cena”,

D – doświadczenie z zakresu szkoleń z cyberbezpieczeństwa

E – wartość punktowa kryterium „Przyjmowanie możliwości wykonania zamówienia poza godzinami 7.30-15.30 tj. przez całą dobę”,

Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.

XVII Wzór umowy

1. Wzór Umowy stanowi Załącznik nr 2 do SWZ.

XVIII RODO

Złożenie oferty stanowi wyraźne działanie potwierdzające wyrażenie zgody przez wykonawcę na przetwarzanie wszystkich tych danych osobowych zawartych w jego ofercie, których przetwarzanie nie może być realizowane przez zamawiającego w oparciu o inne podstawy przetwarzania określone w art. 6.1 RODO.

Zamawiający jest administratorem danych osobowych wykonawcy będącego osobą fizyczną, a także wszelkich osób, których dane wykonawca zawarł w ofercie, gdy ma to zastosowanie.

Dla wykonawcy będącego osobą fizyczną zamawiający przygotował informację o przetwarzaniu jego danych osobowych stanowiącą załącznik nr 5.

Dla osób fizycznych innych niż wykonawca, których dane osobowe wykonawca zawarł w ofercie, zamawiający przygotował informację o przetwarzaniu ich danych osobowych stanowiących załącznik nr 6.

Zamawiający zobowiązuje wykonawcę do przekazania informacji o przetwarzaniu danych osobowych osobom, których dane zawarł w ofercie, gdy ma to zastosowanie.

XX Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej

W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym, a Wykonawcami odbywała się będzie za pośrednictwem Systemu E-Zamówienia Publiczne - zwanego dalej Systemem e-ZP lub Systemem dostępnego pod adresem https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl

Wszelkie informacje dotyczące postępowania w tym zapytania i odpowiedzi dla Wykonawców, modyfikacje SWZ, ogłoszenie wyników itp., będą zamieszczane na Systemie e-ZP.

Przed przystąpieniem do składania oferty, Wykonawca jest zobowiązany zapoznać się z Instrukcją dla wykonawców dot. Systemu E-Zamówienia Publiczne dostępną pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/pomoc oraz Regulaminem korzystania z Systemu E-Zamówienia Publiczne dostępnym pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/regulamin

W postępowaniu o udzielenie zamówienia komunikacja pomiędzy Zamawiającym a Wykonawcami, w szczególności składanie oświadczeń, wniosków (innych niż o dopuszczenie do udziału w postępowaniu),

zawiadomień oraz przekazywanie informacji, odbywa się elektronicznie za pośrednictwem dedykowanych funkcji formularzy „Wiadomość" dostępnych dla każdego zalogowanego Wykonawcy.

Wszelką korespondencję związaną z niniejszym postępowaniem, należy przekazywać za pośrednictwem Systemu e-ZP. Korespondencję uważa się za przekazaną w terminie, jeżeli dotrze do Zamawiającego przed upływem wymaganego terminu. Każda ze stron na żądanie drugiej niezwłocznie potwierdzi fakt otrzymania wiadomości elektronicznej.

Zamawiający wyznacza następującą osobę do kontaktu z Wykonawcami:

• w zakresie dotyczącym przedmiotu zamówienia:

Andrzej Żbikowski za pośrednictwem systemu E-Zamówienia Publiczne,

adres: Gmina Pieńsk, ul. Bolesławiecka 29, 59-930 Pieńsk

• w zakresie dotyczącym zagadnień proceduralnych:

Andrzej Żbikowski za pośrednictwem systemu E-Zamówienia Publiczne,

adres: Gmina Pieńsk, ul. Bolesławiecka 29, 59-930 Pieńsk

Specyfikacja połączenia, formatu przesyłanych danych oraz kodowania i oznaczania czasu odbioru danych Systemu e-ZP:

a) Format kodowania treści w obrębie Systemu - UTF8,

b) Komunikacja pomiędzy przeglądarką Wykonawcy, a serwerem jest wykonywana przy użyciu bezpiecznego protokołu HTTPS,

c) Oznaczeniem czasu odbioru danych przez System jest data oraz dokładny czas (hh: mm: ss) - czas lokalny serwera synchronizowany odpowiednim źródłem czasu.

Wymagania techniczne związane z korzystaniem z Systemu (tj. informacje dotyczące specyfikacji połączenia, formatu przesyłanych danych oraz kodowania i oznaczania czasu przekazania danych):

a) stały dostęp do sieci Internet i minimalna prędkość połączenia internetowego nie mniejsza niż 512 kb/s;

b) zaktualizowana przeglądarka internetowa Chrome w wersji 77 i późniejsze lub Mozilla Firefox w wersji 63 i późniejsze;

c) system operacyjny Microsoft Windows 7 i późniejsze lub Apple macOS 10.14 i późniejsze, dystrybucje systemu Linux;

d) korzystanie z wbudowanej w System e-ZP funkcjonalności składania podpisu elektronicznego możliwe jest pod warunkiem, że system teleinformatyczny, z którego korzysta Wykonawca, wyposażony jest w jeden z poniższych komponentów:

- wirtualna maszyna Java firmy Oracle w wersji co najmniej 1.8.0_221 (Java SE JRE 8 Update 221) z obsługą technologii Java Web Start (JavaWS) lub
- wirtualna maszyna OpenJDK w wersji co najmniej 1.8.0_222 z zainstalowanym rozszerzeniem IcedTea Web Start.

Powyższe wymagania nie ograniczają możliwości korzystania przez Wykonawcę z zewnętrznego oprogramowania do składania podpisu elektronicznego:

a) kwalifikowany podpis elektroniczny (dopuszczalne formaty podpisów: PaDES - format.pdf, XaDES - pozostałe formaty);

b) podpis zaufany;

c) certyfikat osobisty;

d) dopuszczalne formaty danych: .txt, .pdf, .xls, .doc,.docx, .rtf, .odt, .rtf, .xml (zalecany .pdf);

e) maksymalny rozmiar przesyłanych plików złożenia, wycofania oferty oraz wiadomości wynosi 150 MB;

f) w zakresie dotyczącym kodowania i czasu odbioru danych Zamawiający informuje, że złożona przez Wykonawcę za pomocą Systemu e-ZP oferta jest widoczna w systemie, jako zaszyfrowana, a możliwość jej odszyfrowania i otworzenia przez Zamawiającego możliwa jest po upływie terminu składania ofert.

W zależności od formatu podpisu: Podpis kwalifikowany (PAdES, XAdES), podpis osobisty (XAdES), podpis zaufany (PAdES, XAdES) i jego typu (zewnętrzny, otaczający) Wykonawca dołącza do Systemu e-ZP uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z podpisem (typ otaczający).

Sposób sporządzenia dokumentów elektronicznych musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 poz. 2452) oraz rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. z 2020 poz. 2415) oraz rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (załącznik nr 2 do Rozporządzenia).

Wykonawca może zwrócić się do Zamawiającego o wyjaśnienia dotyczące wszelkich wątpliwości związanych z SWZ, przedmiotem zamówienia, sposobem przygotowania i złożenia oferty.

Zamawiający udzieli wyjaśnień zgodnie z art. 284 ustawy Pzp.

Zamawiający umieści wyjaśnienia w Systemie e-ZP bez ujawnienia źródeł zapytania. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ.

Ofertę składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa następnie wraz z plikami stanowiącymi jawną część należy ten plik zaszyfrować.

Do oferty należy dołączyć oświadczenie o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, a następnie zaszyfrować wraz z plikami stanowiącymi ofertę.

Oferta może być złożona tylko do upływu terminu składania ofert.

Wykonawca może przed upływem terminu do składania ofert wycofać ofertę.

Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

XXI Sposób obliczenia ceny

1. Wykonawca poda cenę oferty w Formularzu Ofertowym jako cenę brutto [z uwzględnieniem kwoty podatku od towarów i usług (VAT)] z wyszczególnieniem stawki podatku od towarów i usług (VAT).
2. Cena oferty stanowi wynagrodzenie ryczałtowe.
3. Cena musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
4. Wykonawca poda w Formularzu Ofertowym stawkę podatku od towarów i usług (VAT) właściwą dla przedmiotu zamówienia, obowiązującą według stanu prawnego na dzień składania ofert. Określenie ceny ofertowej z zastosowaniem nieprawidłowej stawki podatku od towarów i usług (VAT) potraktowane będzie, jako błąd w obliczeniu ceny i spowoduje odrzucenie oferty,
5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
6. W przypadku rozbieżności pomiędzy ceną ryczałtową podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena ryczałtowa podana słownie.

XXII Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający zawiera umową w sprawie zamówienia publicznego, z uwzględnieniem art. 577 pzp, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umową w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertą.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o miejscu i terminie podpisania umowy.
4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią Załącznik Nr 2 do SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.
5. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty jako najkorzystniejszej) przedstawią Zamawiającemu umowę regulującą współpracę tych Wykonawców.
6. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

XXIII Środki ochrony prawnej

1. Środki ochrony prawnej przewidziane są w dziale IX ustawy.

2. Środkami ochrony prawnej są odwołanie i skarga do sądu.

3. Środki ochrony prawnej przysługują wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 ustawy Pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.

4 Odwołanie przysługuje na:

1) niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;

2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był

obowiązany na podstawie ustawy;

3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.

23.5 Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, że zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.

6 Terminy wnoszenia odwołań.

1) Odwołanie wnosi się w terminie:

a) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,

b) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a.

7. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej.

8. Odwołanie w przypadkach innych niż określone w pkt 1 i 2 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest mniejsza niż progi unijne.

9. Jeżeli zamawiający nie opublikował ogłoszenia o zamiarze zawarcia umowy lub mimo takiego obowiązku nie przesłał wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty lub nie zaprosił wykonawcy do złożenia oferty w ramach dynamicznego systemu zakupów lub umowy ramowej, odwołanie wnosi się nie później niż w terminie:

1) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania

2) miesiąca od dnia zawarcia umowy, jeżeli zamawiający:

a) nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo

b) zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o wyniku postępowania, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki.

10. Odwołanie zawiera:

1) imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);

2) nazwę i siedzibę zamawiającego, numer telefonu oraz adres poczty elektronicznej zamawiającego;

3) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub NIP odwołującego będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania albo posiada go nie mając takiego obowiązku;

4) numer w Krajowym Rejestrze Sądowym, a w przypadku jego braku - numer w innym właściwym rejestrze, ewidencji lub NIP odwołującego niebędącego osobą fizyczną, który nie ma obowiązku wpisu we właściwym rejestrze lub ewidencji, jeżeli jest on obowiązany do jego posiadania;

5) określenie przedmiotu zamówienia;

6) wskazanie numeru ogłoszenia w przypadku zamieszczenia w Biuletynie Zamówień Publicznych albo publikacji w Dzienniku Urzędowym Unii Europejskiej;

7) wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, lub wskazanie zaniechania przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy;

8) zwięzłe przedstawienie zarzutów;

9) żądanie co do sposobu rozstrzygnięcia odwołania;

10) wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności;

11) podpis odwołującego albo jego przedstawiciela lub przedstawicieli;

12) wykaz załączników.

Do odwołania dołącza się:

1) dowód uiszczenia wpisu od odwołania w wymaganej wysokości;

2) dowód przekazania odpowiednio odwołania albo jego kopii zamawiającemu;

3) dokument potwierdzający umocowanie do reprezentowania odwołującego.

11. Na orzeczenie Izby stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych.

ZAŁĄCZNIKI

Załącznik nr 1 Formularz oferty
Załącznik nr 2 Istotne Postanowienia Umowy
Załącznik nr 3 Oświadczenie wykonawcy
Załącznik nr 4 Oświadczenie o braku powiazań osobowych i kapitałowych
Załącznik nr 5 RODO Pozyskiwanie ofert na usługi dostawy roboty - wykonawcy
Załącznik nr 6 RODO Pozyskiwanie ofert na usługi dostawy roboty - reprezentanci wykonawcy
Załącznik nr 7 Wykaz dostaw
Załącznik nr 8 Wzór oświadczenia o spełnianiu warunków udziału w postępowaniu