

**Szczegółowy opis przedmiotu zamówienia**

# Dostawa systemu zarządzania kontami uprzywilejowanymi

---

## Spis treści

1. Cel zamówienia publicznego. ....	3
2. Słownik użytych pojęć. ....	3
3. Plan komunikacji Wykonawcy z Zamawiającym. ....	3
4. Ogólne wymagania Zamawiającego dotyczące zakresu przedmiotu zamówienia. ....	4
5. Harmonogram realizacji przedmiotu zamówienia ....	4
6. Wymagania Zamawiającego dotyczące dostaw. ....	5
7. Wymagania w zakresie wdrożenia. ....	5
8. Minimalne wymagania dotyczące oferowanego systemu ....	6
9. Minimalne wymagania Zamawiającego w zakresie świadczenia usług wsparcia technicznego producenta. ....	10
10. Minimalne wymagania Zamawiającego dotyczące wytwarzanych i przetwarzanych dokumentów w tym dokumentacji powykonawczej ....	11
11. Minimalne wymagania Zamawiającego w zakresie świadczenia Asysty Technicznej Wykonawcy. ....	12
12. Minimalne wymagania Zamawiającego dotyczące świadczenia usług wynikających z udzielonej gwarancji. ....	13
13. Minimalne wymagania stawiane przez Zamawiającego w zakresie szkolenia administratorów ....	14
14. Minimalne wymagania stawiane przez Zamawiającego w zakresie dwóch szkoleń użytkowników. ....	14
15. Minimalne wymagania stawiane przez Zamawiającego w zakresie jednego/dwóch technicznych warsztatów produktowych w przypadku jego/ich zaoferowania. ....	15
16. Sposób realizacji dostępu zdalnego (spoza siedziby Zamawiającego) na potrzeby realizacji Umowy. ....	15
17. Wzór protokołu odbioru ....	16

## **1. Cel zamówienia publicznego.**

Przedmiotem zamówienia jest dostawa i wdrożenie systemu zarządzania kontami uprzywilejowanymi, oraz świadczenie usług Asysty Technicznej Wykonawcy dla dostarczonego rozwiązania.

## **2. Słownik użytych pojęć.**

- 2.1. System – rozwiązanie sprzętowo-programowe składające się z serwerów fizycznych oraz w razie potrzeby także wirtualnych o wymaganej funkcjonalności opisanej w OPZ wraz z niezbędnymi licencjami.
- 2.2. Wsparcie techniczne producenta - gotowość producenta do świadczenia pomocy w przypadku awarii i problemów technicznych oraz dostęp do bazy wiedzy, dokumentacji, poprawek i nowych wersji oprogramowania.
- 2.3. Awaria - brak działania lub nieprawidłowe działanie Systemu.
- 2.4. Usterka - za usterkę przyjmuje się stan w którym System działa poprawnie jednak czynności administracyjne jak i funkcjonalne są ograniczone z powodu niezależnego od pracowników Zamawiającego a będącego skutkiem niewłaściwego działania systemu lub różnic pomiędzy aktualną konfiguracją a faktycznym działaniem systemu.
- 2.5. Dzień roboczy - liczony od poniedziałku do piątku w godzinach 8:00-16:00 za wyłączeniem dni przypadających w dni wolne od pracy określone w art.1 ust.1 ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (Dz. U. z 2015 r. poz. 90).
- 2.6. Asysta Techniczna Wykonawcy – prace realizowane przez pracowników Wykonawcy w zakresie wdrożonego Systemu obejmujące m.in.: konsultacje techniczne, pomoc w rozwiązywaniu problemów, konfigurację i aktualizację Systemu, przeprowadzanie warsztatów dla jego użytkowników.
- 2.7. Dostawa - dostarczenie elementów składających się na System (sprzęt, licencje itp.) będący przedmiotem zamówienia wraz z dokumentami potwierdzającymi zapewnienie wsparcia technicznego producenta przez wymagany okres.

## **3. Plan komunikacji Wykonawcy z Zamawiającym.**

- 3.1. Możliwe kanały komunikacji to:
  - 3.1.1. Wideokonferencja (obsługę zapewnia Zamawiający),
  - 3.1.2. Telefon,
  - 3.1.3. E-mail,
  - 3.1.4. Spotkanie w siedzibie NIK.
- 3.2. Wszystkie prace będą realizowane przy udziale lub w konsultacji z pracownikami Zamawiającego.
- 3.3. Wykonawca będzie konsultował z Zamawiającym wszystkie przyjmowane założenia poczynione w związku z realizacją umowy. W związku z tym, w razie potrzeby dostarczy wszelkich niezbędnych wyjaśnień i materiałów dodatkowych (opisów, dokumentacji itp.) pracownikom Zamawiającego tak, aby możliwe było jednoznaczne zrozumienie proponowanych przez niego założeń.
- 3.4. Wszystkie ustalenia poczynione za pośrednictwem wideokonferencji, telefonicznie lub w trakcie spotkania muszą zostać niezwłocznie potwierdzone za pośrednictwem wiadomości e-mail. Mogą zostać z nich także sporządzone notatki zgodnie ze wzorem dostarczonym przez Zamawiającego.

- 3.5. Wykonawca zobowiązany jest poinformować Zamawiającego o wszystkich zdarzeniach lub przeszkodach mogących spowodować opóźnienie w wykonaniu Umowy w stosunku do terminów przewidzianych w umowie.

#### **4. Ogólne wymagania Zamawiającego dotyczące zakresu przedmiotu zamówienia.**

- 4.1. Dostawa komponentów zaoferowanego System (sprzęt/oprogramowanie) spełniających minimalne wymagania funkcjonalne Zamawiającego określone w pkt. 8, wraz z **3 letnim wsparciem technicznym producenta licząc od dnia podpisania protokołu odbioru dostawy**.
- 4.2. Wdrożenie (instalacja i konfiguracja) dostarczonego Systemu zgodnie z wymaganiami określonymi w pkt. 7.
- 4.3. Opracowanie i dostarczenie Zamawiającemu dokumentacji powykonawczej zgodnie z wymaganiami określonymi w pkt 10.
- 4.4. Przeprowadzenie przez Wykonawcę szkolenia administratorów zaoferowanego Systemu zgodnie z wymaganiami określonymi w pkt 13.
- 4.5. Przeprowadzenie przez Wykonawcę dwóch szkoleń użytkowników zaoferowanego Systemu zgodnie z wymaganiami określonymi w pkt 14.
- 4.6. Świadczenie Asysty Technicznej Wykonawcy zgodnie z wymaganiami określonymi w pkt 11 od dnia podpisania protokołu odbioru wdrożenia o którym mowa w pkt 7.7 do terminu upływu obowiązywania wsparcia technicznego producenta (o którym mowa w pkt 4.1).
- 4.7. Przeprowadzenie jednego/dwóch technicznych warsztatów produktowych zgodnie z wymaganiami określonymi w pkt 14.<sup>1</sup>

#### **5. Harmonogram realizacji przedmiotu zamówienia**

- 5.1. Dostawa komponentów oraz dokumentów, w których producent potwierdza możliwość korzystania przez Zamawiającego z usług wsparcia technicznego producenta dostarczonego przez Wykonawcę rozwiązania, o którym mowa w pkt. 4.1 w terminie **do .....<sup>2</sup> dni** (maksymalnie 30) licząc od dnia podpisania umowy.
- 5.2. Przeprowadzenie w terminie **14 dni** od dnia podpisania protokołu odbioru dostawy o której mowa w pkt 5.1 wdrożenia (instalacji i konfiguracji) oferowanego rozwiązania zgodnie z wymaganiami określonymi w pkt 7.
- 5.3. Opracowanie i dostarczenie Zamawiającemu dokumentacji powykonawczej wdrożonego rozwiązania w terminie **do 14 dni** od dnia podpisania protokołu odbioru wdrożenia o którym mowa w pkt 7.7.
- 5.4. Przeprowadzenie przez Wykonawcę jednego trzydniowego szkolenia administratorów wdrożonego Systemu, w sposób opisany w pkt 13, w trakcie trwania Asysty Technicznej Wykonawcy.
- 5.5. Przeprowadzenie przez Wykonawcę dwóch jednodniowych szkoleń użytkowników wdrożonego Systemu w sposób opisany w pkt 14, w trakcie trwania Asysty Technicznej Wykonawcy.

---

<sup>1</sup> Punkt będzie obowiązywał w przypadku zaoferowania przez Wykonawcę.

<sup>2</sup> Liczba dni zostanie wpisana na podstawie oferty Wykonawcy (dodatkowe kryterium oceny ofert).

- 5.6. Świadczenie Asysty Technicznej Wykonawcy dla wdrożonego Systemu, w ramach puli **300 godzin** do wykorzystania od momentu podpisania protokołu odbioru wdrożenia (o którym mowa w pkt 7.7) do upływu terminu obowiązywania wsparcia technicznego producenta dostarczonego rozwiązania (o którym mowa w pkt 4.1).
- 5.7. Przeprowadzenie przez Wykonawcę jednego/dwóch technicznych warsztatów produktowych w zakresie wdrożonego systemu w sposób opisany w pkt. 15 w terminach uzgodnionych z Zamawiającym w trakcie trwania Asysty Technicznej Wykonawcy.<sup>3</sup>

## **6. Wymagania Zamawiającego dotyczące dostaw.**

- 6.1. Dostawa musi zostać zrealizowana w terminie wskazanym w pkt 5.1 OPZ.
- 6.2. Miejscem dostawy jest siedziba Najwyższej Izby Kontroli przy ul. Filtrowej 57 w Warszawie.
- 6.3. Koszty dostawy (w tym koszty opakowania, ubezpieczenia, transportu) ponosi Wykonawca.
- 6.4. Dostawa będzie awizowana przez Wykonawcę na piśmie lub e-mailem kierowanym na adres [bit@nik.gov.pl](mailto:bit@nik.gov.pl).
- 6.5. Wszystkie elementy wchodzące w zakres dostawy zostaną dostarczony Zamawiającemu w opakowaniach zabezpieczających przed uszkodzeniem w czasie transportu.
- 6.6. Dostarczone elementy muszą być fabrycznie nowe i nie mogą znajdować się na liście „end-of-sale” lub/oraz „end-of-support” producenta.
- 6.7. Wykonawca zobowiązuje się dostarczyć wymagane urządzenia, oprogramowanie oraz licencje pochodzące z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta na terenie UE i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta na terenie UE.
- 6.8. Potwierdzeniem realizacji dostawy będzie protokół odbioru, podpisany przez przedstawicieli Zamawiającego i Wykonawcy.

## **7. Wymagania w zakresie wdrożenia**

- 7.1. Instalacja Systemu w infrastrukturze Zamawiającego wraz z konfiguracją wysokiej dostępności (klaster Active-Passive lub replikacja typu Disaster Recovery).
- 7.2. Konfiguracja i parametryzacja poszczególnych komponentów systemu.
- 7.3. Konfiguracja oraz synchronizacja z systemami zamawiającego w szczególności:
  - 7.3.1. Active Directory (Windows Server 2012 R2)
  - 7.3.2. Serwer RADIUS (Wheel Cerb)
  - 7.3.3. SIEM (RSA NetWitness),
  - 7.3.4. Remote Desktop Services (Windows Server 2012 R2)

---

<sup>3</sup> Punkt będzie obowiązywał w przypadku zaoferowania przez Wykonawcę.

- 7.4. Konfiguracja kont użytkowników oraz połączeń do systemów docelowych (SSH, RDP, WWW) wraz uprawnieniami dla wybranych użytkowników i automatyczną zmianą hasła na systemie docelowym.
- 7.4.1. Konfiguracja podwójnej autentykacji użytkowników (ang. Two-Factor / Two-Steps) do zaoferowanego rozwiązania przy wykorzystaniu systemów Zamawiającego, w szczególności Active Directory oraz serwera Radius generującego jednorazowe kody SMS.
- 7.4.2. Konfiguracja kont użytkowników jak i połączeń do systemów docelowych rozumiana jest przez Zamawiającego jako możliwość połączenia co najmniej 15 użytkowników do 25 systemów (adresów IP) przy założeniu że na każdym adresie IP może działać więcej niż 1 usługa, np. SSH i WWW lub RDP i WWW, przy założeniu że dostęp do tych usług może odbywać się równolegle oraz wszystkie sesje są nagrywane.
- 7.4.3. Konfiguracja co najmniej 5 połączeń za pomocą aplikacji typu gruby klient lub przeglądarki WWW z wykorzystaniem funkcjonalności RemoteApp usługi Remote Desktop Services dla systemu docelowego, z jednoczesnym nagrywaniem sesji.
- 7.5. Konfiguracja konieczności akceptacji dostępu do wybranych systemów przez użytkowników oraz konieczności akceptacji „podglądu hasła” dla wybranych systemów.
- 7.6. Przygotowanie planu i przeprowadzenie testów akceptacyjnych obejmujących w szczególności:
- 7.6.1. poprawności instalacji, konfiguracji i działania poszczególnych komponentów systemu
- 7.6.2. poprawności działania mechanizmów wysokiej dostępności
- 7.6.3. Sprawdzenie poprawności automatycznej zmiany haseł, nagrywania sesji, połączeń za pomocą klienta WWW.
- 7.7. Zakończeniem wdrożenia będzie protokół odbioru wdrożenia podpisany bez uwag przez obie strony.

## **8. Minimalne wymagania dotyczące oferowanego systemu**

### **8.1. Architektura systemu**

- 8.1.1. Dopuszczalne są następujące warianty architektury systemu:
- a) Jeden serwer fizyczny będący bezpiecznym repozytorium haseł, drugi serwer pracujący w trybie Disaster Recovery na środowisku wirtualnym, pozostałe komponenty Systemu zainstalowane na posiadanym przez Zamawiającego środowisku wirtualnym.
  - b) Dwa dedykowane serwery fizyczne w ramach których zainstalowana jest całość oprogramowania obejmująca system operacyjny, bazę danych, oprogramowanie realizujące pełną funkcjonalność Systemu w trybie wysokiej dostępności rozumianej co najmniej jako klaster Active-Passive.
- 8.1.2. Wykonawca wraz z fizycznymi serwerami dostarczy wszystkie niezbędne do jego pracy licencje obejmujące w szczególności system operacyjny oraz bazę danych wraz z 3 letnim wsparciem technicznym producenta aktualizacji do nowych wersji dla tego oprogramowania od momentu podpisania protokołu odbioru dostawy.
- 8.1.3. Fizyczne serwery muszą spełniać następujące parametry minimalne:
- a) procesor minimum 6 rdzeniowy o częstotliwości taktowania minimum 2,4 GHz

- b) 32 GB pamięci RAM
  - c) Dyski twarde 4 x1 TB (RAID 10 – 2TB)
  - d) Wysokość maksimum 2U
  - e) minimum 3 letnia gwarancja z czasem skutecznej naprawy do końca następnego dnia roboczego od momentu zgłoszenia.
  - f) 4 porty sieciowe 10/100/1000 Mbps
- 8.1.4. System musi dawać możliwość pracy bez konieczności instalacji agenta na systemach docelowych których hasłami będzie zarządzał.
- 8.1.5. Interfejs systemu musi być dostępny w bezpiecznym połączeniu za pośrednictwem przeglądarki internetowej.

## 8.2. Licencjonowanie

Dostarczone wraz z systemem niewyłączne i bezterminowe licencje muszą umożliwiać:

- a) zarządzanie hasłami dla minimum 500 systemów docelowych (adresów IP) bez limitu liczby kont użytkowników Systemu którzy uzyskują dostęp do tych systemów
- lub
- b) Jednoczesną pracę przez co najmniej 75 użytkowników Systemu bez limitu systemów docelowych do których będzie uzyskiwany dostęp.

## 8.3. Integracja

Oferowany System musi dawać możliwość integracji z:

- a) Domeną Active Directory w zakresie kont użytkowników oraz autoryzacji w domenie,
- b) Serwerem RADIUS w celu konfiguracji uwierzytelniania dwu składnikowego i/lub dwu etapowego,
- c) Serwerem Remote Desktop Services w celu umożliwienia dostępu do aplikacji typu gruby klient i dostępnych przez przeglądarkę internetową,
- d) Systemem SIEM (RSA NetWitness) w zakresie przekazywania logów,
- e) Systemem pocztowy Exchange 2012 w zakresie wysyłania powiadomień.

## 8.4. Wspierane systemy docelowe

- 8.4.1. System musi posiadać wsparcie dla zarządzania kontami uprzywilejowanymi dla:
- a) Systemów operacyjnych: Windows Desktop i Server, Windows SSH, MAC OSX, Linux, HP-UX,
  - b) Baz danych: MySQL, Oracle, SQL Server
  - c) Urządzeń: Cisco, Checkpoint, Dell iDRAC, Fortinet, HP iLo, Juniper, Palo Alto Networks
  - d) Mediów społecznościowych: Facebook, Google, Instragram, Twitter

- 8.4.2. System musi dawać możliwość tworzenia połączeń typu SSH do niestandardowych dedykowanych rozwiązań z możliwością ich parametryzacji umożliwiającej prawidłową komunikację z takim systemem.

## **8.5. Zarządzanie hasłami**

- 8.5.1. System musi dawać możliwość definiowania polityk złożoności hasła w zakresie jego długości oraz zawartości (duże litery, małe litery, cyfry, znaki specjalne).
- 8.5.2. System musi generować hasła automatycznie dla kont systemów docelowych zgodnie ze zdefiniowaną polityką złożoności haseł.
- 8.5.3. System musi generować unikalne hasła dla konta systemów docelowych.
- 8.5.4. System musi umożliwiać ręczną (inicjowaną przez administratora) zmianę hasła na wskazanym koncie systemu docelowego.
- 8.5.5. System musi zapewniać możliwość definiowania częstotliwości zmiany hasła na kontach systemów docelowych (codziennie, tygodniowo, miesięcznie).
- 8.5.6. System musi automatycznie zmieniać hasła na wskazanych kontach systemów docelowych zgodnie ze zdefiniowaną polityką częstotliwości zmiany hasła.
- 8.5.7. W przypadku systemów Windows zmianie musi podlegać także hasło w usługach które korzystają z konta dla którego hasło zostało automatycznie zmienione.
- 8.5.8. System musi zapewniać weryfikację zgodności hasła na koncie systemu docelowego z hasłem zapisanym w Systemie ze zdefiniowaną częstotliwością (codziennie, tygodniowo, miesięcznie).
- 8.5.9. System musi posiadać mechanizm automatycznej zmiany haseł na systemach docelowych który będzie ponawiał próby ich zmiany do czasu aż zmiana zakończy się powodzeniem lub zatrzyma się po określonej ilości prób.
- 8.5.10. System musi umożliwiać zapisywanie zdefiniowanej wcześniejszych ilości haseł dla systemów docelowych i ich przeglądanie.

## **8.6. Zarządzanie kluczami RSA i DSA**

- 8.6.1. System musi umożliwiać zdefiniowanie reguł określających typ klucza (RSA lub DSA), długość klucza oraz dawać możliwość ich szyfrowania zgodnie ze zdefiniowaną polityką.
- 8.6.2. System musi umożliwiać automatyczne generowanie kluczy zgodnie ze zdefiniowanymi regułami.
- 8.6.3. System musi umożliwiać zdefiniowanie polityk częstotliwości zmiany kluczy systemów docelowych.

## **8.7. Zarządzanie sesjami**

- 8.7.1. System musi zapewniać możliwość zestawienia sesji do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta w systemie docelowym dla systemów Windows, Unix, Linux.
- 8.7.2. System musi zapewniać zestawienie sesji do systemu docelowego z wykorzystaniem protokołów SSH i RDP.



- 8.7.3. System musi zapewniać blokowanie i zrywanie sesji zestawionych do systemu docelowego przez System przez uprawnionego użytkownika.
- 8.7.4. System musi zapewniać funkcjonalność umożliwiającą zmianę hasła na koncie systemu docelowego po zakończeniu połączenia z tym systemem.
- 8.7.5. System musi dawać możliwość zestawienia sesji SSH do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta w systemie docelowym z wykorzystaniem dowolnego klienta SSH.
- 8.7.6. System musi dawać możliwość zestawienia sesji RDP do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta w systemie docelowym z wykorzystaniem dowolnego klienta RDP.
- 8.7.7. System musi umożliwiać zestawienie połączenia RDP lub SSH z wykorzystaniem dowolnego klienta bez konieczności wcześniejszego logowania się do interfejsu Systemu (z wyłączeniem sytuacji w której skonfigurowane jest logowanie typu dwu składniowego lub dwu etapowego dla użytkownika korzystającego z sesji RDP).

## **8.8. Nagrywanie sesji**

- 8.8.1. System musi zapewniać możliwość nagrywania i podglądu na żywo przez uprawnionych użytkowników sesji zestawianych za pośrednictwem Systemu do systemów docelowych.
- 8.8.2. System musi zapewniać możliwość zablokowania lub zakończenia przez uprawnionych użytkowników aktywnej sesji do systemu docelowego.
- 8.8.3. System musi zapewniać możliwość odtwarzania nagranych wcześniej sesji przez uprawnionych użytkowników Systemu.
- 8.8.4. System musi zapewniać możliwość rejestracji poleceń i ich wyników dla sesji SSH z możliwością wyszukiwania tekstowego.
- 8.8.5. System musi zapewniać możliwość rejestracji aktywności w sesji RDP, uwzględniającej kliknięcia myszą, nazwy otwieranych okien z możliwością wyszukiwania tekstowego.
- 8.8.6. Dla sesji SSH system umożliwia zdefiniowanie poleceń których wydanie spowoduje ich blokadę (brak wykonania), blokadę sesji lub zakończenie sesji do systemu docelowego.

## **8.9. Zarządzanie użytkownikami i grupami**

- 8.9.1. System musi umożliwiać zarządzanie dostępem jego użytkowników do haseł i/lub sesji kont systemów docelowych.
- 8.9.2. System umożliwia łączenie jego użytkowników w grupy w celu uproszczenia procesu nadawania uprawnień.

## **8.10. Dostęp do sesji lub haseł**

- 8.10.1. System musi umożliwiać złożenie wniosku o dostęp do hasła i/lub sesji do systemu docelowego, przy założeniu automatycznej akceptacji lub akceptacją jednopoziomowej przez jednego lub wielu uprawnionych operatorów.
- 8.10.2. System musi umożliwiać wysłanie powiadomienia email do użytkownika wnioskującego o dostęp do hasła i/lub sesji w przypadku zakończenia procesu zatwierdzania.

- 8.10.3. System musi umożliwiać określenie rodzaju dostępu jaki może uzyskać określony użytkownik (hasło do konta, nawiązanie sesji RDP/SSH).

### **8.11. Separacja uprawnień**

- 8.11.1. System musi dawać możliwość separacji uprawnień w zakresie:
- a) Administratora Systemu zarządzania kontami uprzywilejowanymi,
  - b) Administratora systemu docelowego uzyskującego dostęp lub wnioskującego o dostęp do systemu docelowego lub do hasła umożliwiającego taki dostęp,
  - c) Zatwierdzającego wnioski o dostęp do systemu docelowego lub hasło do niego,
  - d) Audytora mającego dostęp do monitoringu i przeglądania sesji oraz logów.

### **8.12. Raportowanie i audyt**

- 8.12.1. System musi umożliwiać generowanie raportów automatyczne oraz „na żądanie”.
- 8.12.2. System musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy jego użytkowników.
- 8.12.3. System musi umożliwiać rejestrację i raportowanie procesu wnioskowania o dostęp do hasła i/lub sesji.
- 8.12.4. System musi umożliwiać rejestrację i raportowanie każdej aktywności związanej z kontem systemu docelowego, a w szczególności zmianę hasła na takim koncie i pobranie hasła do takiego konta.

### **8.13. Licencje zapewniane przez Zamawiającego**

- 8.13.1. W ramach posiadanego środowiska wirtualnego Zamawiający zapewni w razie potrzeby następujące licencje dla oferowanego przez Wykonawcę systemu:
- a) Windows Server 2012/2016 Standard/Datacenter – dowolna ilość,
  - b) Licencje Windows Remote Desktop Services (istniejący serwer RDS w infrastrukturze Zamawiającego) do 30 jednoczesnych sesji.

## **9. Minimalne wymagania Zamawiającego w zakresie świadczenia usług wsparcia technicznego producenta.**

- 9.1. Wsparcie techniczne producenta musi obejmować:

- 9.1.1. zapewnienie dostępu do bazy wiedzy o Systemie,
- 9.1.2. zapewnienie dostępu do dokumentacji i oprogramowania Systemu,
- 9.1.3. zapewnienie dostępu do forum technicznego,
- 9.1.4. zapewnienie dostępu do poprawek i nowych wersji oprogramowania Systemu,
- 9.1.5. telefoniczne wsparcie techniczne w dni robocze w godzinach 8-16,

9.1.6. czas reakcji do 2 godzin od momentu zgłoszenia.

**10. Minimalne wymagania Zamawiającego dotyczące wytwarzanych i przetwarzanych dokumentów w tym dokumentacji powykonawczej**

10.1. Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji projektu charakteryzowały się wysoką jakością, w szczególności:

10.1.1. czytelną i zrozumiałą strukturą zarówno poszczególnych dokumentów jak i całej dokumentacji z podziałem na rozdziały podrozdziały i sekcje,

10.1.2. zachowaniem standardów oraz sposobu pisanie, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów, oraz fragmentów tego samego dokumentu jak również całej dokumentacji.

10.2. Wykonawca przygotowuje dokumentację powykonawczą szczegółowo opisującą wszystkie zrealizowane prace instalacyjne i konfiguracyjne wraz ze schematem podłączenia Systemu w infrastrukturze Zamawiającego.

10.3. W ramach dokumentacji powykonawczej Wykonawca dostarczy procedury i instrukcje administracyjne, obejmujące w szczególności:

10.3.1. wykonanie kopii bezpieczeństwa Systemu i jego odtworzenie,

10.3.2. aktualizację i wdrażania poprawek,

10.3.3. procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,

10.3.4. diagnozowanie systemu i jego komponentów,

10.3.5. sprawdzanie wydajności poszczególnych komponentów system,

10.3.6. sprawdzanie poprawności działania trybu wysokiej dostępności i/lub Disaster Recovery wdrożonego Systemu,

10.3.7. konfigurację: kont użytkowników, dodawania systemów, podglądu/hasła, tworzenia nowych połączeń, zmiany harmonogramu rotacji hasła,

10.3.8. konfigurację parametrów nagrywania sesji,

10.4. Każda z procedur powinna zawierać co najmniej następujące dane:

- a) nazwa,
- b) opis,
- c) częstotliwość wykonywania,
- d) kroki do zrealizowania w procedurze,

- e) informacje (o ile są znane, jeśli jest ich dużo to przykłady bądź wzorce) na jakie należy zwrócić uwagę w trakcie wykonywania procedury,
- f) omówienie zawartości komunikatów jeśli są prezentowane,
- g) kroki jakie należy podjąć w przypadku natknięcia się na nietypowe sytuacje.

10.5. Dokumentacja musi być weryfikowana i w razie potrzeby aktualizowana podczas prac serwisowych Wykonawcy określonych w ramach Asysty Technicznej Wykonawcy.

10.6. Zamawiający wymaga, aby cała dokumentacja, o której mowa powyżej, podlegała jego akceptacji.

## **11. Minimalne wymagania Zamawiającego w zakresie świadczenia Asysty Technicznej Wykonawcy.**

- 11.1. Wykonawca będzie świadczył w terminie wskazanym w pkt 4.6 Asystę Techniczną w zakresie obsługi zgłoszeń, przez certyfikowanego inżyniera w obszarze wdrożonego systemu, w formie elektronicznej i telefonicznej w dni robocze, w języku polskim.
- 11.2. Asysta Techniczna wykonywana w siedzibie Zamawiającego w Warszawie przy ul. Filtrowej 57 będzie realizowana na sprzęcie udostępnionym przez Zamawiającego.
- 11.3. Czas reakcji Wykonawcy na otrzymane zgłoszenie wynosi 4 godziny. W przypadku zgłoszenia serwisowego otrzymanego po godzinie 16.00, czas reakcji liczy się od godziny 8.00 następnego dnia roboczego.
- 11.4. Wykonawca będzie w imieniu Zamawiającego eskalował do producenta danego systemu wszystkie zgłoszenia serwisowe, monitorował i uczestniczył w ich rozwiązywaniu.
- 11.5. Czas rozwiązania zgłoszonego problemu wynosi do 8 godzin w dni robocze. Jeżeli do rozwiązania problemu niezbędne jest udzielenie odpowiedzi przez producenta wówczas czas rozwiązania problemu wynosi do 24 godzin w dni robocze. Czas realizacji zgłoszenia liczony jest od momentu jego wysłania przez Zamawiającego.
- 11.6. Asysta Techniczna Wykonawcy będzie rozliczana zgodnie ze złożoną ofertą Wykonawcy w zależności od faktycznie przepracowanych godzin, rozliczanych zgodnie ze stawką godzinową zawartą w ofercie.
- 11.7. Możliwa do wykorzystania ilość godzin pracy inżyniera w ramach Asysty Technicznej wynosi 300 godzin.
- 11.8. Celem wizyty w ramach Asysty Technicznej mogą być: wszelkie prace związane z systemem objętym usługą, m.in. aktualizacja dokumentacji technicznej i oprogramowania, analiza poprawności działania wdrożonego systemu i jego komponentów, dostrojenie, konfiguracja nowych połączeń/kont użytkowników, rekonfiguracja pozostałych parametrów systemu, przeprowadzanie warsztatów i szkoleń w zakresie funkcjonalności Systemu.
- 11.9. Potwierdzeniem wykonania wizyty w siedzibie Zamawiającego, wykonania zleconych prac i czasu wykorzystanego na daną wizytę będzie protokół odbioru Asysty Technicznej Wykonawcy podpisany przez obie strony.
- 11.10. Czas wizyty przeznaczony na wykonanie Asysty Technicznej Wykonawcy liczony jest od chwili przystąpienia do pracy certyfikowanego inżyniera w obszarze danego rozwiązania w siedzibie Zamawiającego.
- 11.11. Zgłoszenie serwisowe uważa się za otwarte po przesłaniu go przez Zamawiającego do Wykonawcy faksem lub mailem.
- 11.12. Każde zgłoszenie serwisowe rozliczane będzie co do ilości godzin, zgodnie z faktycznym czasem, jaki zajęło rozwiązanie problemu.
- 11.13. Przyjmuje się, że każda rozmowa telefoniczna, wykonywana w ramach Asysty Technicznej, niezależnie od jej rzeczywistego czasu trwania to 15 minut zegarowych.

- 11.14. Przyjmuje się, że każda pojedyncza wiadomość e-mail przesłana przez Wykonawcę do Zamawiającego, w ramach Asysty Technicznej to 15 minut zegarowych.
- 11.15. Po zrealizowaniu zgłoszenia serwisowego Wykonawca poinformuje drogą elektroniczną (e-mail) Zamawiającego o zrealizowaniu tego zgłoszenia serwisowego.
- 11.16. Czas związany z obsługą awarii danego Systemu jak i kontakty z producentem rozwiązania w kwestii usuwania awarii czy usterek nie wlicza się do płatnych godzin Asysty Technicznej.

## **12. Minimalne wymagania Zamawiającego dotyczące świadczenia usług wynikających z udzielonej gwarancji.**

- 12.1. Wykonawca udziela gwarancji od zakończenia wdrożenia do upływu okresu gwarancji producenta, na prawidłowe w pełni zgodne z jego przeznaczeniem, funkcjonowanie systemu zarządzania kontami uprzywilejowanymi.
- 12.2. Naprawa gwarancyjna systemu zostanie dokonana:
  - 12.2.1. po uprzedniej nieodpłatnej ocenie zgłoszonej awarii. Ocena zgłoszonej awarii musi zostać dokonana przez wykwalifikowanego przedstawiciela wykonawcy, w miejscu użytkowania systemu,
  - 12.2.2. w celu przystąpienia do naprawy przedstawiciel służb serwisowych Wykonawcy zgłosi się do miejsca użytkowania systemu. Jeśli naprawa w siedzibie Zamawiającego nie jest możliwa, Wykonawca odbierze uszkodzony element systemu i dostarczy po naprawie na własny koszt i na własną odpowiedzialność,
  - 12.2.3. po zwrocie naprawionego elementu systemu nastąpi sprawdzenie poprawności funkcjonowania całego systemu.
- 12.3. W przypadku wystąpienia awarii komponentów Systemu czas jego niedostępności (brak możliwości zalogowania się do niego jak również za jego pośrednictwem) nie może przekraczać 4 godzin licząc od momentu zgłoszenia awarii do Wykonawcy.
- 12.4. W przypadku awarii sprzętu fizycznego jego wymiana/napraw musi nastąpić w ciągu 1 dnia roboczego od momentu zgłoszenia. Wszystkie czynności związane zgłoszeniem awarii, odbiorem/dostarczeniem sprzętu i jego wymiany obsługuje Wykonawca.
- 12.5. W przypadku awarii uszkodzone dyski pozostają u Zamawiającego i nie podlegają zwrotowi czy wymianie.
- 12.6. Czas usunięcia nieprawidłowości wskazanych w zgłoszeniu gwarancyjnym wynosi do 5 Dni Roboczych od daty zgłoszenia gwarancyjnego pod rygorem naliczania kar umownych na zasadach określonych w Umowie i może ulec wydłużeniu wyłącznie za pisemną zgodą Zamawiającego w przypadku wystąpienia okoliczności niezależnych od Wykonawcy i Zamawiającego.
- 12.7. W przypadku urządzeń i/lub oprogramowania wchodzących w skład Systemu, o którym mowa w pkt 4.1 Wykonawca zapewni świadczenie usług gwarancyjnych przez producenta urządzenia zgodnie z warunkami opisanymi w warunkach gwarancji producenta.
- 12.8. W trakcie trwania umowy Zamawiającego z Wykonawcą usługi gwarancyjne producenta dla posiadanych przez Zamawiającego urządzeń i oprogramowania, wchodzących w skład Systemu, świadczone będą za pośrednictwem Wykonawcy.
- 12.9. W przypadku wystąpienia wad w opracowanych dokumentach, o których mowa w pkt 10, Zamawiający ma prawo żądać ich usunięcia w terminie 7 Dni Roboczych od daty zawiadomienia Wykonawcy (naniesienie uzupełnień i poprawek na wszystkich egzemplarzach dostarczonych Zamawiającemu), pod rygorem naliczania kar umownych na zasadach określonych w Umowie.
- 12.10. Uprawnienia z tytułu rękopisów za wady dokumentacji technicznej wygasają wraz z upływem okresu Asysty Technicznej Wykonawcy.

- 12.11. Udzielone gwarancje nie mogą ograniczać praw Zamawiającego do użytkowania systemu, zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego.

### **13. Minimalne wymagania stawiane przez Zamawiającego w zakresie szkolenia administratorów**

- 13.1. Wykonawca zorganizuje szkolenie z wdrożonego Systemu, dla jednej grupy administratorów, składającej się maksymalnie 5 osób, w ośrodku szkoleniowym producenta lub Wykonawcy na terenie Warszawy, lub w siedzibie Zamawiającego w Warszawie.
- 13.2. Termin i miejsce szkolenia zostanie uzgodnione z Zamawiającym z co najmniej dwutygodniowym wyprzedzeniem.
- 13.3. Szkolenie musi trwać minimum 3 dni robocze, 6 godzin dziennie efektywnych zajęć prowadzonych w języku polskim. W przypadku zaoferowania dodatkowej funkcjonalności skanowania podatności szkolenie musi trwać minimum 4 dni robocze.
- 13.4. Szkolenie musi być prowadzone przez certyfikowanego inżyniera Wykonawcy lub producenta zaoferowanego systemu.
- 13.5. Program szkolenia musi być zgodny z wykorzystywaną przez Zamawiającego wersją systemu oraz obejmować całość zagadnień związanych z czynnościami administracyjnymi zaoferowanego systemu w tym:
- 13.5.1. konfiguracja,
  - 13.5.2. zarządzanie,
  - 13.5.3. monitorowanie,
  - 13.5.4. raportowanie,
  - 13.5.5. omówienie najczęściej występujących awarii oraz sposoby ich usuwania i zabezpieczania się przed nimi.

### **14. Minimalne wymagania stawiane przez Zamawiającego w zakresie dwóch szkoleń użytkowników**

- 14.1. Wykonawca zorganizuje dwa szkolenia z wdrożonego Systemu, każde dla grupy użytkowników składającej się maksymalnie 10 osób, w ośrodku szkoleniowym producenta lub Wykonawcy na terenie Warszawy, lub w siedzibie Zamawiającego w Warszawie.
- 14.2. Termin i miejsce szkolenia zostanie uzgodnione z Zamawiającym z co najmniej dwutygodniowym wyprzedzeniem.
- 14.3. Szkolenie musi trwać minimum 1 dzień roboczy, 6 godzin dziennie efektywnych zajęć prowadzonych w języku polskim.
- 14.4. Szkolenie musi być prowadzone przez certyfikowanego inżyniera Wykonawcy lub producenta zaoferowanego systemu.
- 14.5. Program szkolenia musi być zgodny z wykorzystywaną przez Zamawiającego wersją systemu oraz obejmować całość zagadnień związanych z czynnościami administracyjnymi zaoferowanego systemu w tym:
- 14.5.1. Obsługa interfejsu programu,
  - 14.5.2. zarządzanie własnymi ustawieniami (profilu użytkownika), połączeniami,

- 14.5.3. sposoby nawiązywania połączeń,
- 14.5.4. rozwiązywanie podstawowych problemów oraz ich diagnostyka.

**15. Minimalne wymagania stawiane przez Zamawiającego w zakresie jednego/dwóch technicznych warsztatów produktowych w przypadku jego/ich zaoferowania (dodatkowe kryterium oceny ofert)<sup>4</sup>**

- 15.1. Wykonawca zorganizuje techniczne warsztaty produktowe z zaoferowanego i wdrożonego Systemu, dla jednej grupy administratorów/użytkowników, składającej się maksymalnie z 10 osób, w siedzibie Zamawiającego.
- 15.2. Termin i miejsce technicznego warsztatu produktowego zostanie uzgodnione z Zamawiającym z co najmniej dwutygodniowym wyprzedzeniem.
- 15.3. Techniczny warsztat produktowy musi trwać minimum 1 dzień roboczy, 6 godzin dziennie efektywnych zajęć prowadzonych w języku polskim.
- 15.4. Techniczny warsztat produktowy musi być prowadzone przez certyfikowanego inżyniera Wykonawcy lub producenta zaoferowanego systemu.
- 15.5. Techniczny warsztat produktowy musi dotyczyć tej samej lub nowszej wersji zaoferowanego Systemu oraz obejmować zagadnienia związane z:
  - 15.5.1. czynnościami administracyjnymi zaoferowanego systemu,
  - 15.5.2. zmianami/różnicami występującymi pomiędzy aktualną a nową wersją zaoferowanego systemu,
  - 15.5.3. zmianami/różnicami występującymi pomiędzy aktualną konfiguracją a docelową oczekiwaną przez Zamawiającego.

**16. Sposób realizacji dostępu zdalnego (spoza siedziby Zamawiającego) na potrzeby realizacji Umowy**

- 16.1. Zdalny dostęp będzie realizowany za pośrednictwem rozwiązania udostępnianego przez Zamawiającego i na zasadach przez niego określonych.
- 16.2. Zdalny dostęp do Systemu będzie przyznany wyłącznie w celu wykonywania prac wynikających z niniejszej umowy.
- 16.3. Wykonawca przekaże Zamawiającemu listę pracowników wraz z niezbędnymi danymi określonymi każdorazowo przez Zamawiającego (w szczególności: imię, nazwisko, adres e-mail, nr telefonu komórkowego oraz dane jednoznacznie identyfikujące komputer z którego będzie uzyskiwany dostęp) do konfiguracji zdalnego dostępu.
- 16.4. Zamawiający przekaże Wykonawcy warunki techniczne jakie muszą spełniać komputery Wykonawcy wykorzystywane do zdalnego dostępu; warunki te mogą być przez Zamawiającego modyfikowane w trakcie realizacji umowy po uprzednim powiadomieniu Wykonawcy.
- 16.5. Zamawiający zastrzega sobie możliwość ograniczenia ilości osób którym przyznany zostanie zdalny dostęp.
- 16.6. Pracownicy Wykonawcy którym przyznany został zdalny dostęp zobowiązani są do nie przekazywania danych umożliwiających jego uzyskanie (w szczególności są to: adres systemu, login, hasło, kody jednorazowe) osobom trzecim.

---

<sup>4</sup> Punkt będzie obowiązywał w przypadku zaoferowania przez Wykonawcę.

- 16.7. Zamawiający zastrzega sobie możliwość nagrywania wszystkich czynności realizowanych przez pracowników Wykonawcy za pośrednictwem zdalnego dostępu.
- 16.8. W przypadku czasowej niedostępności zdalnego dostępu z przyczyn niezależnych od Wykonawcy lub Zamawiającego prace wynikające z niniejszej umowy będą realizowane przez pracowników Wykonawcy, w siedzibie Zamawiającego.
- 16.9. Wykonawca zobowiązany jest każdorazowo do wcześniejszego uzgodnienia z upoważnionymi pracownikami Zamawiającego zakresu prac realizowanych za pośrednictwem zdalnego dostępu.
- 16.10. Wykonawca zobowiązuje się do podjęcia wszelkich niezbędnych działań, w tym organizacyjnych i technicznych, mających na celu zabezpieczenie sprzętu za pomocą, którego pracownicy Wykonawcy będą realizowali prace za pośrednictwem zdalnego dostępu.

## **17. Wymagania dla sieciowego skanera podatności (dodatkowe kryterium oceny ofert)**

- 17.1. Skaner musi być zintegrowany z systemem zarządzania kontami uprzywilejowanymi.
- 17.2. Musi umożliwiać wykrywanie urządzeń sieciowych, baz danych i systemów w środowisku wirtualnym.
- 17.3. Musi umożliwiać identyfikację podatności w wykrytych urządzeniach sieciowych, systemach operacyjnych, aplikacjach, baz danych (Oracle, MS SQL, MySQL), portach i usługach za pośrednictwem skanowanie agentowego lub bez agentowego w oparciu o aktualizowaną na bieżąco bazę podatności.
- 17.4. Musi umożliwiać automatyczną ocenę podatności dla aplikacji webowych w zakresie co najmniej OWASP Top Ten.
- 17.5. Musi umożliwiać skany środowiska wirtualnego vmware dla hostów ESXi oraz dla maszyn wirtualnych
- 17.6. Musi mieć możliwość wykorzystania poświadczeń zapisanych w systemie zarządzania kontami uprzywilejowanymi do przeprowadzenia skanowania podatności.
- 17.7. Musi oceniać ryzyko wykrytych podatności i określać priorytety ich usuwania bazując na wskaźnikach określających możliwość ich wykorzystania na podstawie danych z zewnętrznych źródeł jak np. Metasploit, Exploit-db, CVSS itd.
- 17.8. Musi dawać możliwość potwierdzenia istnienia podatności za pomocą testów penetracyjnych z wykorzystaniem np. Metasploit Framework.
- 17.9. Musi posiadać konsolę zarządzającą umożliwiającą dostęp do wyników skanowania podatności, raportowania postępów skanowania i ich wyników.
- 17.10. Musi umożliwiać przekazywanie danych do systemów klasy SIEM (minimum syslog).
- 17.11. Musi umożliwiać wykonywanie skanowania ad-hoc dla podanych adresów IP i zakresów tych adresów.

## **18. Wzór protokołu odbioru**



**Protokół odbioru .....\*)**

Na podstawie Umowy z dnia .....**2018r.**

..... zwan(y/a) dalej Wykonawcą

przekazuje **Najwyższej Izbie Kontroli** zwanej dalej Zamawiającym przedmiot odbioru w postaci:

.....  
.....  
.....  
.....

Zamawiający przyjmuje przedmiot odbioru **bez uwag / z uwagami \*\*)**:

.....  
.....  
.....  
.....

Niniejszy protokół odbioru, sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze Stron.

Warszawa dnia .....2018 r.

Odbierający (NIK)	Przekazujący
.....	.....
(czytelny podpis)	(czytelny podpis)

\*) wpisać rodzaj protokołu odbioru np. odbioru dostawy/odbioru końcowego/odbioru usługi, itp.

\*\*) niepotrzebne skreślić