SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

Zamawiający: Skarb Państwa – Urząd Komunikacji Elektronicznej

Znak sprawy: **BA.WZP.26.44.2022**

Przedmiot zamówienia:

Uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze Zamawiającego

Rozdział 1 – Nazwa i adres Zamawiającego

Skarb Państwa – Urząd Komunikacji Elektronicznej (UKE), ul. Giełdowa 7/9, 01-211 Warszawa.

Osoba uprawniona do kontaktów z Wykonawcami: Łukasz Sobczuk, tel. 22 534 92 95.

Adres strony internetowej Zamawiającego: https://uke.gov.pl

Dostęp do dokumentów można uzyskać pod adresem: https://bip.uke.gov.pl/zamowienia-publiczne/

Skrzynka poczty elektronicznej: zamowienia.publiczne@uke.gov.pl

Rozdział 2 – Ochrona danych osobowych

1. Klauzula informacyjna z art. 13 RODO związana z niniejszym postępowaniem o udzielenie zamówienia publicznego

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.), dalej „RODO", Zamawiający informuje, że:

1) Administratorem Pani/Pana danych osobowych jest Prezes Urzędu Komunikacji Elektronicznej, adres siedziby: ul. Giełdowa 7/9, 01-211 Warszawa, numer telefonu: +48 22 33 04 000, numer faksu: +48 22 53 49 162.
2) Dane kontaktowe Inspektora ochrony danych osobowych w Urzędzie Komunikacji Elektronicznej: adres e-mail: iod@uke.gov.pl.
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z prowadzeniem postępowania o udzielenie zamówienia publicznego w trybie podstawowym bez przeprowadzenia negocjacji pn. **Uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze Zamawiającego – sprawa BA.WZP.26.44.2022.**
4) Podstawą przetwarzania danych osobowych jest ustawa Pzp.
5) Odbiorcami danych osobowych są podmioty uprawnione na mocy obowiązujących przepisów prawa, w szczególności osoby lub podmioty, którym zostanie udostępniona dokumentacja postępowania na podstawie art. 18 oraz art. 74–76 ustawy Pzp. Zasada jawności ma zastosowanie do wszystkich danych osobowych, z wyjątkiem danych, o których mowa w art. 9 ust. 1 RODO (szczególne kategorie danych osobowych).

   Ponadto dane osobowe mogą być udostępniane podmiotom upoważnionym do odbioru danych na podstawie odpowiednich przepisów prawa (np. organy administracji, sądy, służby państwowe), podmiotom, które przetwarzają dane osobowe w imieniu Zamawiającego na podstawie zawartej z nim umowy powierzenia przetwarzania danych osobowych (np. podmioty obsługujące systemy teleinformatyczne Zamawiającego), a także innym administratorom przetwarzającym dane we własnym imieniu (np. podmioty prowadzące działalność pocztową lub kurierską).
6) Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do przeprowadzenia postępowania o udzielenie zamówienia publicznego, a w stosunku do danych osobowych wskazanych przez Wykonawcę, którego oferta została wybrana - przez okres trwania umowy o zamówienie, ale nie krócej niż 4 lata, od dnia zakończenia postępowania o udzielenie

zamówienia publicznego oraz do czasu przedawnienia ewentualnych roszczeń wynikających z umowy. Ponadto dane osobowe będą przechowywane do celów archiwalnych przez okres przewidziany w przepisach kancelaryjno-archiwalnych Zamawiającego, przyjętych zgodnie z ustawą o narodowym zasobie archiwalnym i archiwach.

7) Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp.

8) Posiada Pani/Pan prawo:

   a) uzyskania potwierdzenia, czy Prezes UKE przetwarza Pana/Pani dane osobowe, a jeżeli ma to miejsce uzyskanie na podstawie art. 15 RODO dostępu do treści danych oraz informacji dotyczących takiego przetwarzania; w przypadku gdy wykonanie tego obowiązku, wymagałoby niewspółmiernie dużego wysiłku, Zamawiający może, zgodnie z art. 75 ustawy Pzp, żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia,

   b) uzyskania kopii danych osobowych,

   c) żądania na podstawie art. 16 RODO sprostowania lub uzupełnienia danych osobowych; zgodnie z art. 76 ustawy Pzp wykonanie tego obowiązku nie może naruszać integralności protokołu postępowania oraz jego załączników,

   d) żądania na podstawie art. 18 RODO ograniczenia przetwarzania danych osobowych; zgodnie z art. 74 ust. 3 ustawy Pzp wykonanie tego obowiązku nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia.

9) W trakcie przetwarzania Pani/Pana danych osobowych nie dochodzi do zautomatyzowanego podejmowania decyzji ani do profilowania, o których mowa w art. 22 ust. 1 RODO.

10) Posiada Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

Rozdział 3 – Tryb udzielenia zamówienia

1. Postępowanie prowadzone jest w trybie podstawowym bez przeprowadzenia negocjacji, na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710) – dalej „ustawą Pzp".
2. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.

Rozdział 4 – Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze Zamawiającego, które obejmuje w szczególności:
   1) wykonanie Analizy środowiska Zamawiającego oraz sporządzenie Projektu Technicznego;
   2) uruchomienie i konfiguracja rozwiązania PAM w najnowszej dostępnej wersji;
   3) udzielenie lub zapewnienie udzielenia licencji/subskrypcji dla oprogramowania PAM na warunkach producenta wraz z gwarancją i usługą wsparcia technicznego na okres 12 miesięcy, w tym:

a. możliwość pracy 20 administratorów będących pracownikami Zamawiającego oraz
b. możliwość pracy 50 kontraktorów (zewnętrznych dostawców)

4) przeprowadzenie instruktażu dla Zamawiającego z uruchomienia, konfiguracji i administracji PAM;
5) sporządzenie i dostarczenie Zamawiającemu Dokumentacji Powykonawczej;
6) merytoryczne wsparcie administratorów rozwiązania PAM w ilości 160 godzin w okresie 12 miesięcy, licząc od dnia podpisania Końcowego Protokołu Odbioru.

Szczegółowo Przedmiot Umowy został określony w Załączniku nr 1 do SWZ.

2. Wspólny słownik zamówień (CPV):

Kod wg Wspólnego Słownika Zamówień	Nazwa wg Wspólnego Słownika Zamówień
72260000-5	Usługi w zakresie oprogramowania
72246000-1	Usługi doradcze w zakresie systemów

3. Wykonawca zapewni odpowiednią liczbę osób i środków, aby w sposób niezakłócony i należyty realizować zamówienie.

4. Na podstawie art. 95 ust. 1 ustawy, Zamawiający wymaga od Wykonawcy lub podwykonawcy, aby co najmniej jedna osoba pełniąca nadzór nad realizacją umowy (pełniąca funkcję Koordynatora odpowiedzialnego za prawidłową realizację zamówienia) była zatrudniona na podstawie umowy o pracę przez cały okres trwania umowy, w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. - Kodeks Pracy (Dz.U. z 2022 r. poz. 1510). Szczegóły opisane zostały we wzorze umowy stanowiącym Załącznik nr 5 do SWZ.

   Do zadań osoby pełniącej funkcję Koordynatora należało będzie w szczególności udzielanie natychmiastowej pomocy, jeśli pojawią się wątpliwości lub trudności przy realizacji zamówienia. Koordynator będzie udzielał Zamawiającemu wszelkich informacji związanych z organizacją wykonywanych usług w każdej sytuacji, gdy powstanie potrzeba przekazania uwag, wyjaśnienia wątpliwości, czy powzięcia przez Zamawiającego informacji o niezgodnych z warunkami umowy działaniach Wykonawcy. Koordynator dostępny będzie pod telefonem komórkowym i adresem e-mail. Koordynator na bieżąco będzie monitorował realizację obsługi zgłoszeń przekazanych przez osoby uprawnione oraz będzie kontrolował prawidłowość realizacji zamówienia przez Wykonawcę.

5. Realizacja pozostałych czynności niezbędnych do wykonania przedmiotu zamówienia nie wymaga występowania pomiędzy Wykonawcą lub podwykonawcą i zatrudnionymi przez te podmioty osobami podporządkowania w rozumieniu przepisów prawa pracy.

6. Zamawiający informuje, że ewentualne podane w opisie przedmiotu zamówienia nazwy własne nie mają na celu naruszenia art. 99 ustawy Pzp, a mają jedynie za zadanie sprecyzowanie oczekiwań jakościowych i technologicznych Zamawiającego. Zamawiający dopuszcza rozwiązania równoważne pod warunkiem spełnienia tego samego poziomu technologicznego, wydajnościowego i funkcjonalnego przedmiotu zamówienia. Wszystkie ewentualne nazwy własne i marki handlowe zawarte w SWZ oraz dokumentacji, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego. Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w dokumentacji przetargowej mogą być zastąpione urządzeniami bądź materiałami równoważnymi. Poprzez pojęcie materiałów i urządzeń równoważnych należy rozumieć materiały gwarantujące realizację dostaw lub usług zgodnie z wymaganiami Zamawiającego oraz zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w dokumentacji przetargowej i specyfikacji

technicznej.

7. Wykonawca zobowiązany jest zrealizować zamówienie na zasadach i warunkach opisanych w projekcie umowy stanowiącym Załącznik nr 6 do SWZ.

INFORMACJE DODATKOWE

1. Postępowanie prowadzone jest w języku polskim.
2. Zamawiający nie dopuszcza składania ofert częściowych.

   Powody niedokonania podziału zamówienia na części:

   Zamówienie jest niepodzielne w rozumieniu art. 25 ust. 2 ustawy Pzp. Powodem niedokonania podziału zamówienia na części jest to, że przedmiotowe zamówienie, którego przedmiotem jest uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze Zamawiającego oraz wsparcie merytoryczne jest jednorodne i nie występuje bowiem sytuacja w której poszczególni Wykonawcy mogliby wykonywać różne rodzaje zadań. Podział zamówienia spowodowałby wydłużenie jego realizacji oraz trudności w zakresie skorelowania działań poszczególnych Wykonawców. Jednocześnie przedmiot zamówienia należy traktować jako jedną całość, tym samym nie ma możliwości podziału zamówienia na części.

   W ocenie Zamawiającego brak podziału zamówienia na części oraz wielkość zamówienia nie jest na tyle znacząca, więc nie utrudni małym lub średnim przedsiębiorcom wzięcia w nim udziału.
3. Zamawiający nie dopuszcza składania ofert wariantowych.
4. Zamawiający nie przewiduje zawarcia umowy ramowej.
5. Zamawiający nie przewiduje możliwości udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.
6. Zamawiający nie przewiduje możliwości ani wymogu odbycia wizji lokalnej lub sprawdzenia przez Wykonawców dokumentów niezbędnych do realizacji zamówienia dostępnych na miejscu u Zamawiającego, o których mowa w art. 131 ust. 2 ustawy Pzp.
7. Rozliczenia pomiędzy Zamawiającym a Wykonawcą będą prowadzone w PLN. Zamawiający nie przewiduje rozliczania w walutach obcych.
8. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu (z zastrzeżeniem przepisu art. 261 ustawy Pzp).
9. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej po dokonaniu oceny ofert w celu wyboru najkorzystniejszej oferty.
10. Zamawiający nie przewiduje obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań, a Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).
11. 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 znane na tym etapie) nazwy (firmy) tych podwykonawców.
12. Zamawiający nie przewiduje wymogu ani możliwości złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93 ustawy Pzp.
13. Zamawiający przewiduje możliwość dokonania zmian umowy na warunkach określonych we

wzorze Umowy.

14. Zamawiający nie zastrzega wymogów ani wymagań związanych z realizacją zamówienia, o których mowa odpowiednio w art. 94 i 96 ustawy Pzp.

Rozdział 5 – Przedmiotowe środki dowodowe

Zamawiający nie wymaga złożenia przedmiotowych środków dowodowych.

Rozdział 6 – Termin wykonania zamówienia

Wymagany termin realizacji zamówienia: **do dnia 20.12.2022 r.**.

Wykonawca zobowiązany jest do dostarczenia Zamawiającemu dokumentu wystawiony przez Producenta/dystrybutora potwierdzający zapewnienie Zamawiającemu prawa do licencji/subskrypcji oraz gwarancji i usługi wsparcia technicznego w terminie do 20.12.2022 r..

Rozdział 7 – Podstawy wykluczenia, o których mowa w art. 108 oraz 109 ustawy Pzp

1. Zamawiający wykluczy Wykonawcę z postępowania, w przypadkach wskazanych w przepisie art. 108 ust. 1 ustawy Pzp oraz przepisie art. 109 ust. 1 pkt 1, 4, 5 i 7 ustawy Pzp.
2. W przypadku, o którym mowa przepisie art. 109 ust. 1 pkt 1 i pkt 4 ustawy Pzp, Zamawiający może nie wykluczać Wykonawcy, jeżeli wykluczenie byłoby w sposób oczywisty nieproporcjonalne, w szczególności, gdy kwota zaległych podatków lub składek na ubezpieczenie społeczne jest niewielka, albo sytuacja ekonomiczna lub finansowa Wykonawcy, o którym mowa w art. 109 ust. 1 pkt. 4 ustawy, jest wystarczająca do wykonania zamówienia.
3. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.
4. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 4 ustawy Pzp, jeżeli udowodni Zamawiającemu, że spełnił łącznie następujące przesłanki:
   1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;
   2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;
   3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
      a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,
      b) zreorganizował personel,
      c) wdrożył system sprawozdawczości i kontroli,

d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,

e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.

5. Zamawiający oceni, czy podjęte przez Wykonawcę czynności, o których mowa w ust. 4, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy. Jeżeli podjęte przez Wykonawcę czynności, o których mowa w ust. 4, nie są wystarczające do wykazania jego rzetelności, Zamawiający wykluczy Wykonawcę.
6. Zamawiający wskazuje, że okresy wykluczenia zostały wskazane w przepisie art. 111 ustawy Pzp.

Rozdział 8 – Podstawy wykluczenia, o których mowa w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego

1. Zamawiający wykluczy z niniejszego postępowania:
   1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
   2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
   3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.
2. Wzór oświadczenia dot. przesłanek wykluczenia z art. 7 ust. 1 ustawy sankcyjnej składanego na podstawie art. 125 ust. 1 ustawy Pzp stanowi Załącznik nr 6 do SWZ.

Rozdział 9 – Warunki udziału w postępowaniu

Zamawiający nie stawia szczegółowych warunków udziału w postępowaniu.

Rozdział 10 – Oświadczenia i dokumenty, jakie zobowiązani są dostarczyć Wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu oaz wykazania braku podstaw wykluczenia (podmiotowe środki dowodowe)

1. **DOKUMENTY SKŁADANE RAZEM Z OFERTĄ:**

   1) **Oświadczenie dotyczące braku podstaw wykluczenia z postępowania**.

Oświadczenie to stanowi dowód potwierdzający brak podstaw wykluczenia – wzór stanowi Załącznik nr 3 do SWZ;

Oświadczenie, o którym mowa wyżej składają odrębnie:

a) Wykonawca/każdy spośród Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

b) podwykonawcy, jako oświadczenie potwierdzające brak podstaw wykluczenia podwykonawców (jeżeli dotyczy).

2) **Pełnomocnictwo** (jeżeli dotyczy):

a) gdy umocowanie osoby składającej ofertę nie wynika z dokumentów potwierdzających umocowanie do reprezentowania, Wykonawca, który składa ofertę za pośrednictwem pełnomocnika, powinien dołączyć do oferty dokument pełnomocnictwa obejmujący swym zakresem umocowanie do złożenia oferty lub do złożenia oferty i podpisania umowy. Obowiązek ten stosuje się odpowiednio do osoby działającej w imieniu podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy Pzp lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach,

b) w przypadku Wykonawców ubiegających się wspólnie o udzielenie zamówienia Wykonawcy zobowiązani są do ustanowienia pełnomocnika. Dokument pełnomocnictwa, z treści którego będzie wynikało umocowanie do reprezentowania w postępowaniu o udzielenie zamówienia tych Wykonawców należy załączyć do oferty,

c) pełnomocnictwa powinny być załączone do oferty i powinny zawierać w szczególności wskazanie:

- postępowania o zamówienie publiczne, którego dotyczy,
- wszystkich Wykonawców ubiegających się wspólnie o udzielenie zamówienia wymienionych z nazwy z określeniem adresu siedziby lub nazwy z określeniem adresu siedziby podmiotu udostępniającego zasoby lub nazwy z określeniem adresu siedziby podwykonawcy niebędącego podmiotem udostępniającym zasoby,
- ustanowionego pełnomocnika oraz zakresu jego umocowania.

3) **Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia** (jeżeli dotyczy) – Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane. W takiej sytuacji Wykonawcy są zobowiązani wypełnić oświadczenie w Załączniku nr 2 do SWZ – Formularz ofertowy, z którego wynika, które usługi wykonają poszczególni Wykonawcy;

4) **Zastrzeżenie tajemnicy przedsiębiorstwa** (jeżeli dotyczy) – w sytuacji, gdy oferta lub inne dokumenty składane w toku postępowania będą zawierały tajemnicę przedsiębiorstwa, Wykonawca, wraz z przekazaniem takich informacji, zastrzega, że nie mogą być one udostępniane, oraz wykazuje poprzez dołączenie uzasadnienia, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;

5) **oświadczenie na potwierdzenie braku podstaw wykluczenia z art. 7 ust. 1 ustawy sankcyjnej**, zgodnie ze wzorem określonym w Załączniku nr 7 do SWZ.

DOKUMENTY SKŁADANE NA WEZWANIE (WYKAZ PODMIOTOWYCH ŚRODKÓW DOWODOWYCH)

Zamawiający wzywa Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w

wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych, aktualnych na dzień złożenia.

1. **Podmiotowe środki dowodowe wymagane od Wykonawcy obejmują:**
   1) **Oświadczenie Wykonawcy**, w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp, o braku przynależności do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej – Załącznik nr 4 do SWZ;
   2) **odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej**, w zakresie art. 109 ust. 1 pkt. 4 ustawy Pzp, sporządzonych nie wcześniej, niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.
2. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 4 zastępuje się je w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy.
3. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli:
   1) może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2021 poz. 670), o ile Wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp dane umożliwiające dostęp do tych środków,
   2) podmiotowym środkiem dowodowym jest oświadczenie, którego treść odpowiada zakresowi oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp.
4. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
5. W zakresie nieuregulowanym ustawą Pzp lub niniejszą SWZ do oświadczeń i dokumentów składanych przez Wykonawcę w postępowaniu zastosowanie mają w szczególności przepisy Rozporządzenia Ministra Rozwoju Pracy i Technologii z dnia 30 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać Zamawiający od Wykonawcy (Dz.U. 2020 poz. 2415) oraz Rozporządzenia 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. 2020 poz. 2452).
6. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania, wezwać Wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych aktualnych na dzień ich złożenia – art. 274 ust 2 ustawy Pzp.

Rozdział 11 – 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

1. Komunikacja w postępowaniu o udzielenie zamówienia i w konkursie, w tym składanie ofert, wniosków o dopuszczenie do udziału w postępowaniu lub konkursie, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między Zamawiającym a Wykonawcą, z uwzględnieniem wyjątków określonych w ustawie Pzp, odbywa się przy użyciu środków komunikacji elektronicznej. Przez środki komunikacji elektronicznej rozumie się środki komunikacji elektronicznej zdefiniowane w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344).
2. Komunikacja między Zamawiającym a Wykonawcami odbywać się będzie drogą elektroniczną przy użyciu:
   1) Portalu e-Zamówienia: https://ezamowienia.gov.pl/pl/
   2) Poczty elektronicznej, e-mail: zamowienia.publiczne@uke.gov.pl

   Wszelkie dokumenty związane z prowadzonym postępowaniem zamieszczane będą na stronie Zamawiającego tj. https://bip.uke.gov.pl/zamowienia-publiczne/
3. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów 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.
4. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.
5. Zamawiający nie ponosi odpowiedzialności z tytułu nieotrzymania przez Wykonawcę informacji związanych z prowadzonym postępowaniem w przypadku wskazania przez Wykonawcę w ofercie np. błędnego adresu poczty elektronicznej.
6. Wykonawca może w formie elektronicznej zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ. Zamawiający niezwłocznie udzieli wyjaśnień jednak nie później niż 2 dni przed upływem terminu składania ofert – pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynie do Zamawiającego nie później niż na 4 dni przed upływem wyznaczonego terminu składania ofert i nie dotyczy udzielonych wyjaśnień.
7. Wnioski o wyjaśnienie treści SWZ należy przesyłać za pośrednictwem Portalu e-Zamówienia (https://ezamowienia.gov.pl/pl/) lub za pomocą poczty elektronicznej na adres e-mail: zamowienia.publiczne@uke.gov.pl .

   W temacie korespondencji należy podać numer i nazwę postępowania. Treść wniosków wraz z wyjaśnieniami Zamawiający zamieści na stronie internetowej (https://bip.uke.gov.pl/zamowienia-publiczne/ oraz https://ezamowienia.gov.pl/pl/), bez ujawniania źródła wniosku.
8. W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu składania ofert zmodyfikować treść niniejszej SWZ.
9. Każda wprowadzona przez Zamawiającego zmiana stanie się częścią SWZ. Dokonaną zmianę treści SWZ Zamawiający udostępni na stronie internetowej prowadzonego postępowania.
10. Zamawiający przedłuży termin składania ofert, jeżeli w wyniku modyfikacji treści SWZ niezbędny

będzie dodatkowy czas na wprowadzenie zmian w ofertach.

11. Osobą upoważnioną przez Zamawiającego do kontaktowania się z Wykonawcami jest **Łukasz Sobczuk tel. +48 22 534 92 95** - e-mail: zamowienia.publiczne@uke.gov.pl
12. Wykonawca zamierzający wziąć udział w niniejszym postępowaniu musi posiadać konto podmiotu „Wykonawca" na Platformie e-Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej https://ezamowienia.gov.pl oraz informacje zamieszczone w zakładce „Centrum Pomocy".
13. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie e-Zamówienia ani logowania.
14. Komunikacja w postępowaniu, z wyłączeniem składania ofert, odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce „Formularze" („Formularze do komunikacji") lub poczty elektronicznej. Za pośrednictwem „Formularzy do komunikacji" lub poczty elektronicznej odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk „dodaj załącznik").
15. Możliwość korzystania w postępowaniu z „Formularzy do komunikacji" w pełnym zakresie wymaga posiadania konta „Wykonawcy" na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia.
16. Do korzystania z „Formularzy do komunikacji" służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie e-Zamówienia.
17. Wszystkie wysłane i odebrane w postępowaniu przez wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce „Komunikacja".
18. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji" wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
19. Maksymalny łączny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250 MB.
20. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia.
21. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu (32) 77 88 999 lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej https://ezamowienia.gov.pl w zakładce „Zgłoś problem".

Rozdział 12 – Termin związania ofertą

1. Wykonawca będzie związany ofertą przez okres **30 dni, tj. do dnia 27 grudnia 2022 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.

3. Przedłużenie terminu związania ofertą wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

Rozdział 13 – Opis sposobu przygotowania ofert oraz wymagania formalne dotyczące składanych oświadczeń i dokumentów

1. Oferta musi obejmować całość przedmiotu zamówienia i musi być sporządzona zgodnie z wymogami określonymi niniejszą SWZ.
2. Wykonawca ma prawo złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej rozwiązania alternatywne lub oferty wariantowej, spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.
3. Oferta oraz wszelkie dokumenty wymagane w niniejszej SWZ muszą spełniać następujące wymogi:
   1) oferta musi zostać sporządzona w języku polskim z zachowaniem formy pisemnej na komputerze, ręcznie czytelnym pismem, Zamawiający nie wyraża zgody na złożenie wymaganych dokumentów w innym języku niż język polski bez stosownego tłumaczenia. Dokumenty (w tym oświadczenia) sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski (tłumaczenie zwykłe) - oryginał tłumaczenia lub kopia tłumaczenia poświadczona za zgodność z oryginałem przez Wykonawcę. W razie wątpliwości wersja polskojęzyczna jest wersją wiążącą;
   2) Formularz oferty i wszystkie załączane dokumenty sporządzone przez Wykonawcę (również te złożone na załączonych do SWZ wzorach) muszą być podpisane w formie elektronicznej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez osobę(-y) upoważnioną(-e) do reprezentowania zgodnie z formą reprezentacji Wykonawcy, określoną w dokumencie rejestrowym lub innym dokumencie, właściwym dla formy organizacyjnej;
   3) w przypadku, gdy Wykonawcę reprezentuje pełnomocnik do oferty musi być załączone pełnomocnictwo określające jego zakres i podpisane przez osoby uprawnione do reprezentacji Wykonawcy;
   4) osoba (osoby) składająca(e) oświadczenie ponosi odpowiedzialność za treść złożonego oświadczenia na zasadach określonych w art. 297 § 1 kodeksu karnego;
4. W przypadku złożenia przez Wykonawców oferty wspólnej, Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i do zawarcia umowy w sprawie zamówienia publicznego. Oryginał pełnomocnictwa musi być załączony do oferty.
5. Załączony do oferty oryginał pełnomocnictwa powinien zawierać w szczególności wskazanie:
   1) postępowania o zamówienie publiczne, którego dotyczy,
   2) wszystkich Wykonawców ubiegających się wspólnie o udzielenie zamówienia, wymienionych z nazwy, z określeniem adresu siedziby,
   3) ustanowionego pełnomocnika oraz zakres jego umocowania.
6. Dokument pełnomocnictwa musi być podpisany przez wszystkich Wykonawców ubiegających się wspólnie o udzielenie zamówienia, w tym pełnomocnika. Podpisy muszą być złożone przez osoby uprawnione do składania oświadczeń woli wymienione we właściwym rejestrze lub ewidencji Wykonawców.

7. Oświadczenia, formularze, dokumenty sporządzone na załączonych do SWZ wzorach muszą być podpisane przez pełnomocnika.
8. Ofertę składa i podpisuje w imieniu wszystkich Wykonawców, pełnomocnik, wpisując w miejscu przeznaczonym na podanie nazwy i adresu Wykonawcy, nazwy i adresy wszystkich Wykonawców składających ofertę wspólną z zaznaczeniem pełnomocnika.
9. Składając ofertę, powołując się na Wykonawcę, w miejscu np. nazwa i adres Wykonawcy, należy wpisać dane dotyczące wszystkich Wykonawców występujących wspólnie, a nie pełnomocnika.
10. Wszelka korespondencja prowadzona będzie wyłącznie z pełnomocnikiem.
11. Jeżeli oferta Wykonawców występujących wspólnie zostanie wybrana, Zamawiający może zażądać przed zawarciem umowy w sprawie zamówienia publicznego, pisemnej umowy regulującej współpracę tych Wykonawców która zawierać będzie w szczególności: wskazanie stron konsorcjum, cel zawarcia umowy, okres obowiązywania umowy, wskazanie Lidera Konsorcjum (pełnomocnika), wskazania obowiązków i uprawnień Lidera Konsorcjum, zakres obowiązków poszczególnych członków konsorcjum, wskazanie udziału w zyskach i ponoszeniu strat przez poszczególnych członków Konsorcjum, klauzule solidarnej odpowiedzialności członków Konsorcjum za należyte wykonanie umowy, wskazanie podmiotu (Lidera Konsorcjum) upoważnionego do wystawiania faktur VAT na Zamawiającego z tytułu należnego wynagrodzenia.
12. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ponoszą solidarną odpowiedzialność za wykonanie umowy.
13. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku o nazwie: „Załącznik stanowiący tajemnicę przedsiębiorstwa", a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum .zip. Wykonawca zobowiązany będzie, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego, jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji, zgodnie z postanowieniami art. 18 ust. 3 ustawy Pzp.

    Uwaga: Zastrzegając informacje w ofercie Wykonawca winien mieć na względzie, że zastrzeżona informacja ma charakter tajemnicy przedsiębiorstwa, jeśli spełnia poniższe warunki, określone w art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji tj.: ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub posiada wartość gospodarczą, oraz jako całość lub w szczególnym zestawieniu i zbiorze elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji, albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzenia nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.

    W nawiązaniu do orzecznictwa arbitrażowego i sądowego, należy przyjąć, iż sferą tajemnicy można objąć tylko takie informacje, które są znane jedynie poszczególnym osobom lub określonej grupie osób. Obszar ten nie może się rozciągać na informacje powszechnie znane lub te, o których treści każdy zainteresowany może się legalnie dowiedzieć.
14. Zamawiający informuje, że w przypadku kiedy Wykonawca otrzyma od niego wezwanie w trybie art. 224 ustawy Pzp, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą

tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich, jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie Zamawiający uzna za skuteczne wyłącznie w sytuacji kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

15. Wykonawca w szczególności nie może zastrzec w ofercie informacji:
    1) przekazywanych po otwarciu ofert, o których mowa w art. 222 ust. 5 ustawy Pzp,
    2) które są jawne na mocy odrębnych przepisów,
    3) cen jednostkowych stanowiących podstawę wyliczenia ceny oferty.
16. Wszelkie negatywne konsekwencje mogące wyniknąć z niezachowania powyższych wymagań będą obciążały Wykonawcę.
17. Do przygotowania oferty zaleca się wykorzystanie Formularza oferty, którego wzór stanowi Załącznik nr 2 do SWZ. W przypadku, gdy Wykonawca nie korzysta z przygotowanego przez Zamawiającego wzoru, w treści oferty należy zamieścić wszystkie informacje wymagane w Formularzu oferty.

Rozdział 14 – Sposób oraz termin składania ofert

1. Ofertę należy złożyć w formie elektronicznej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym za pośrednictwem https://ezamowienia.gov.pl/pl/ **do dnia 28 listopada 2022 r. do godz. 11:00.**
2. Sposób złożenia, zmiany i wycofania oferty został opisany w „Instrukcji dla Wykonawcy" dostępnej pod adresem internetowym: https://ezamowienia.gov.pl
3. O terminie złożenia oferty decyduje czas pełnego przeprocesowania transakcji na Platformie e-Zamówienia. Czas, którym znakowany jest złożony dokument pochodzi z niezależnego źródła, jakim jest dostawca.
4. Wykonawca może złożyć tylko jedną ofertę.

Rozdział 15 – Termin otwarcia ofert

1. Otwarcie ofert nastąpi w dniu składania ofert **28 listopada 2022 r. o godz. 12:00** za pośrednictwem Platformy e-Zamówienia.
2. W przypadku awarii Platformy e-Zamówienia, która spowoduje brak możliwości otwarcia ofert w ww. terminie, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
3. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informacje o:
    1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
    2) cenach lub kosztach zawartych w ofertach.

Rozdział 16 – Sposób obliczenia ceny

1. Cenę należy rozumieć jako cenę w rozumieniu art. 3 ust. 1 pkt 1 i ust. 2 ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług (Dz.U. z 2019 r. poz. 178 z późn. zm.).
2. Wykonawca przedstawi cenę oferty brutto w Formularzu ofertowym (Załącznik nr 1 do SWZ).
3. Cenę oferty należy określić z dokładnością do drugiego miejsca po przecinku, zgodnie z zasadami rachunkowości.
4. Kwoty należy zaokrąglić do pełnych groszy, przy czym końcówki poniżej 0,5 grosza pomija się, a końcówki 0,5 i wyższe zaokrągla się do 1 grosza (ostatnią pozostawioną cyfrę powiększa się o jednostkę), zgodnie z art. 106e ust. 11 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2021 r., poz. 685, z późn. zm.).
5. Podana w Formularzu ofertowym cena musi uwzględniać wszystkie koszty, jakie poniesie Wykonawca z tytułu należytej realizacji przedmiotu zamówienia, zgodnej z warunkami wynikającymi z SWZ i Opisu Przedmiotu Zamówienia oraz wzoru Umowy. Cena winna również uwzględniać wysokość minimalnego wynagrodzenia za pracę oraz wysokość minimalnej stawki godzinowej w 2022 r. wynikające z ROZPORZĄDZENIA RADY MINISTRÓW z dnia 14 września 2021 r. w sprawie wysokości minimalnego wynagrodzenia za pracę oraz wysokości minimalnej stawki godzinowej w 2022 r.
6. Zamawiający zastrzega, że cena za realizację przedmiotu zamówienia wskazana przez Wykonawcę w Formularzu ofertowym, a także żadna cena jednostkowa nie może mieć wartości 0,00 złotych.
7. Jeżeli Wykonawca złoży ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje Zamawiającego w Formularzu ofertowym (Załącznik nr 2 do SWZ), czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
8. Sposób zapłaty i rozliczenia za realizację zamówienia, określone zostały we wzorze Umowy.

Rozdział 17 – Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Oferty zostaną ocenione przez Zamawiającego w oparciu o następujące kryteria i ich znaczenie:

Kryterium	Znaczenie procentowe kryterium	Maksymalna liczba punktów jakie może otrzymać oferta za kryterium
Cena (C)	90,00 %	90,00 punktów
Czas reakcji (R)	10,00 %	10,00 punktów

2. Zasady oceny:

   1) W kryterium „Cena” (C).

      W przypadku kryterium „Cena”, oferta otrzyma zaokrągloną do dwóch miejsc po przecinku liczbę punktów wynikającą z działania:

$$\boldsymbol{P_i(C)} = \frac{\boldsymbol{C_{min}}}{\boldsymbol{C_i}} \cdot \boldsymbol{max(C)}$$

      gdzie:

      i – numer oferty;

      $\boldsymbol{P_i(C)}$ – liczba punktów jakie otrzyma oferta „i” za kryterium „Cena (C)”;

      $\boldsymbol{C_{min}}$ – najniższa cena brutto spośród wszystkich nieodrzuconych ofert;

      $\boldsymbol{C_i}$ – cena brutto oferty „i” (oferty badanej);

      $\boldsymbol{max(C)}$ – maksymalna liczba punktów jakie może otrzymać badana oferta za kryterium „Cena (C)” – 90 punktów.

   2) W kryterium „Czas reakcji” (R).

      Ocena oferty w ramach tego kryterium będzie dokonywana na podstawie wypełnionego Formularza Ofertowego stanowiącego Załącznik nr 2 do SWZ, w którym Wykonawca zobowiązany będzie do wskazania maksymalnego czasu reakcji na zgłoszenie w ramach merytorycznego wsparcia administratorów.

      W zależności od wskazanego przez Wykonawcę oferowanego czasu reakcji, Zamawiający przyzna Wykonawcy odpowiednią liczbę punktów:

      - powyżej 48 h – 0 pkt
      - powyżej 24 h i nie więcej niż 48 h – 5 pkt,
      - do 24 h – 10 pkt.

      W przypadku, gdy Wykonawca nie wpisze w Formularzu Ofertowym (Załącznik nr 2 do SWZ) oferowanego czasu reakcji, zastosowanie w takiej sytuacji będzie miał maksymalny czas reakcji, tj. powyżej 48 h. W takim przypadku oferta otrzyma za kryterium oceny ofert „Czas reakcji" – 0 (zero) punktów.

3. Wybór oferty najkorzystniejszej.

   Za ofertę najkorzystniejszą zostanie uznana oferta, która przy uwzględnieniu powyższych kryteriów i ich wag otrzyma najwyższą punktację obliczoną jako suma punktów otrzymanych za poszczególne kryteria oceny ofert.

   Jeżeli nie będzie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybiera ofertę z najniższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wzywa Wykonawców, którzy złożyli oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen lub kosztów wyższych niż zaoferowane w złożonych ofertach.

Rozdział 18 – Zabezpieczenie należytego wykonania umowy

Zamawiający nie wymaga zabezpieczenia należytego wykonania umowy.

Rozdział 19 – Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający preferuje zawarcie umowy w formie elektronicznej (w postaci elektronicznej z kwalifikowanym podpisem elektronicznym). W przypadku braku możliwości podpisania umowy w formie elektronicznej, umowa może być zawarta w formie pisemnej.
2. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza, jest zobowiązany, do podpisania umowy na warunkach określonych w SWZ oraz w miejscu (w przypadku umowy zawieranej w formie pisemnej) i terminie wyznaczonym przez Zamawiającego.
3. Dokumenty, jakich może zażądać Zamawiający przed zawarciem umowy:
   1) pełnomocnictwo dla osób podpisujących umowę, jeśli ich umocowanie do podpisania umowy nie wynika z dokumentów złożonych w postępowaniu;
   2) w przypadku wyboru oferty Wykonawców wspólnie ubiegających się o udzielenie zamówienia – kopię umowy regulującej współpracę tych podmiotów, w tym również umowy spółki cywilnej. Wykonawcy ponoszą solidarną odpowiedzialność za wykonanie umowy.
4. Zamawiający informuje, że:
   1) niedopełnienie przez Wykonawcę formalności, o których mowa w ust. 3 albo
   2) dwukrotne niestawienie się Wykonawcy na wezwanie Zamawiającego do podpisania umowy w formie pisemnej albo
   3) niezwrócenie we wskazanym przez Zamawiającego terminie podpisanej przez Wykonawcę umowy w formie elektronicznej,

   - zostanie przez Zamawiającego uznane za uchylanie się Wykonawcy od zawarcia umowy, w rozumieniu art. 263 ustawy Pzp.

Rozdział 20 – Projektowane postanowienia, które zostaną wprowadzone do umowy w sprawie zamówienia publicznego

Z Wykonawcą, którego oferta będzie wybrana jako najkorzystniejsza, zostanie podpisana umowa, której projekt stanowi Załącznik nr 6 do SWZ.

Rozdział 21 – Wymagania w zakresie zatrudnienia na podstawie stosunku pracy, w okolicznościach, o których mowa w art. 95 ust. 1 ustawy

1. Zamawiający wymaga zatrudnienia przez wykonawcę lub podwykonawcę, na podstawie umowy o pracę, osobę nadzorującą realizację zamówienia, tj. pełniąca funkcję Koordynatora odpowiedzialnego za prawidłową realizację zamówienia.
2. W trakcie realizacji zamówienia, w każdym przypadku powzięcia wiadomości o braku respektowania zatrudnienia na umowę o pracę, Zamawiający uprawniony jest do wykonywania czynności kontrolnych wobec Wykonawcy odnośnie spełniania przez Wykonawcę lub podwykonawcę wymogu

zatrudnienia na podstawie umowy o pracę wyżej wymienionych osób. Zamawiający uprawniony jest w szczególności do:

1) żądania oświadczeń i dokumentów w zakresie potwierdzenia spełniania ww. wymogów i dokonywania ich oceny,
2) żądania wyjaśnień w przypadku wątpliwości w zakresie potwierdzenia spełniania ww. wymogów,
3) przeprowadzania kontroli na miejscu wykonywania świadczenia.

3. W trakcie realizacji zamówienia na każde wezwanie Zamawiającego w wyznaczonym w tym wezwaniu terminie Wykonawca przedłoży Zamawiającemu wskazane poniżej dowody w celu potwierdzenia spełnienia wymogu zatrudnienia na podstawie umowy o pracę przez Wykonawcę lub Podwykonawcę wyżej wymienionych osób w trakcie realizacji zamówienia:
   1) oświadczenie Wykonawcy lub Podwykonawcy o zatrudnieniu na podstawie umowy o pracę osoby wykonującej czynności, których dotyczy wezwanie Zamawiającego. Oświadczenie to powinno zawierać w szczególności: dokładne określenie podmiotu składającego oświadczenie, datę złożenia oświadczenia, wskazanie, że objęte wezwaniem czynności wykonuje osoba zatrudniona na podstawie umowy o pracę wraz ze wskazaniem tej osoby, imię i nazwisko tej osoby, rodzaju umowy o pracę i wymiaru etatu oraz podpis osoby uprawnionej do złożenia oświadczenia w imieniu Wykonawcy lub Podwykonawcy;
   2) poświadczoną za zgodność z oryginałem odpowiednio przez Wykonawcę lub Podwykonawcę kopię umowy/umów o pracę osoby wykonującej w trakcie realizacji zamówienia czynności, których dotyczy ww. oświadczenie Wykonawcy lub Podwykonawcy (wraz z dokumentem regulującym zakres obowiązków, jeżeli został sporządzony). Kopia umowy/umów powinna zostać zanonimizowana w sposób zapewniający ochronę danych osobowych pracownika, zgodnie z art. 5 ust. 1 lit. c RODO, tj. w szczególności bez adresu, nr PESEL pracownika. Imię i nazwisko pracownika nie podlega anonimizacji. Informacje takie jak: data zawarcia umowy, rodzaj umowy o pracę i wymiar etatu powinny być możliwe do zidentyfikowania;
   3) zaświadczenie właściwego oddziału ZUS, potwierdzające opłacanie przez Wykonawcę lub Podwykonawcę składek na ubezpieczenia społeczne i zdrowotne z tytułu zatrudnienia na podstawie umów o pracę za ostatni okres rozliczeniowy;
   4) poświadczoną za zgodność z oryginałem odpowiednio przez Wykonawcę lub Podwykonawcę kopię dowodu potwierdzającego zgłoszenie pracownika przez pracodawcę do ubezpieczeń, zanonimizowaną w sposób zapewniający ochronę danych osobowych pracowników, zgodnie z art. 5 ust. 1 lit. c RODO. Imię i nazwisko pracownika nie podlega anonimizacji.
4. Z tytułu niespełnienia przez Wykonawcę lub Podwykonawcę wymogu zatrudnienia na podstawie umowy o pracę pracowników Zamawiający przewiduje sankcję w postaci obowiązku zapłaty przez Wykonawcę kary umownej w wysokości określonej w projekcie umowy stanowiącej Załącznik nr 5 do SWZ. Niezłożenie przez Wykonawcę w wyznaczonym przez Zamawiającego terminie żądanych przez Zamawiającego dowodów w celu potwierdzenia spełnienia przez Wykonawcę lub Podwykonawcę wymogu zatrudnienia na podstawie umowy o pracę traktowane będzie, jako niespełnienie przez Wykonawcę lub Podwykonawcę wymogu zatrudnienia na podstawie umowy o pracę pracowników.
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.

Rozdział 22 – Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy

Wykonawcom przysługują środki ochrony prawnej zgodnie z Działem IX ustawy Pzp.

Rozdział 23 – Załączniki do SWZ

Załącznik nr 1 –	Opis przedmiotu zamówienia;
Załącznik nr 2 –	Wzór formularza ofertowego;
Załącznik nr 3 –	Oświadczenie dotyczące braku podstaw wykluczenia z postępowania;
Załącznik nr 4 –	Wzór oświadczenia o przynależności albo braku przynależności do tej samej grupy kapitałowej (art. 108 ust. 1 pkt 5 ustawy Pzp);
Załącznik nr 5 –	Wzór oświadczenia, o którym mowa w art. 117 ust. 4 ustawy Pzp (dotyczy wykonawców wspólnie ubiegających się o udzielenie zamówienia);
Załącznik nr 6 –	Projekt Umowy;
Załącznik nr 7 –	Wzór oświadczenia dot. przesłanek wykluczenia z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego składane na podstawie art. 125 ust. 1 ustawy Pzp.

Szczegółowy opis przedmiotu zamówienia.

1. Opis funkcjonalny Privileged Access Management (PAM):

Zarządzanie kontami i dostępami uprzywilejowanymi

1.1 Oprogramowanie musi posiadać funkcje zarządzania (automatycznej zmiany haseł, definiowania polityki dostępu) kontami uprzywilejowanymi w:

a) Systemach operacyjnych: Windows, Unix, Linux (Debian, Ubuntu, RedHat), pSeries (AIX),
b) Bazach danych: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, DB2, MariaBD, MongoDB, PostgreSQL,
c) Systemach zarządzania infrastrukturą, aplikacjach: DELL DRAC, IBM Tivoli, RSA authentication Manager, HP iLO, SAP Application Server, MDM,
d) Urządzeniach sieciowych oraz systemach bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint, Netscreen, F5, Infoblox NIOS, FireEye Malware Analysis, FortiGate, Palo Alto Networks,
e) Narzędziach CI/CD: Chef, Jenkins, Kubernetes, Docker,
f) Aplikacjach typu SaaS/ stronach web/ interfejach web, minimum takich jak: Amazon Web Services (klucze API oraz konta uprzywilejowane, konto root), Zarządzanie Microsoft Azure (klucze API oraz konta uprzywilejowane),
g) Modułach: Microsoft Services, Scheduled tasks, IIS application Pool, IIS Directory Security, w rejestrach, COM+ , zarządzanie kontami w domenie Microsoft,
h) Plikach konfiguracyjnych, tabelach baz danych,
i) Środowiskach wirtualizacyjnych VMWare ESX/ESXi.

1.2 Oprogramowanie musi zapewniać wsparcie (ochronę kont) dla dowolnego urządzenia obsługującego ODBC w wersji 2.7 lub wyższej.

1.3 Oprogramowanie musi zapewniać wsparcie (możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego) dla systemów spoza listy "out of box" z wykorzystaniem skryptów lub innych mechanizmów realizowanych i wspieranych przez producenta rozwiązania dostępnych nieodpłatnie na oficjalnej stronie producenta rozwiązania. Producent powinien udostępniać nie mniej niż 200 unikalnych integracji udostępnionych w ramach wspomnianego portalu.

1.4 W przypadku ochrony kont lokalnych administratorów na stacjach roboczych Windows oraz MAC OS proponowane oprogramowanie musi obsługiwać scenariusz potencjalnej niedostępności stacji w momencie wykonania polityki automatycznej zmiany hasła lokalnego administratora (realizowanej przez narzędzie ochrony kont). W przypadku systemów, które często znajdują się poza siecią lokalną Zamawiającego musi istnieć możliwość wykorzystania narzędzia / agenta instalowanego na stacji roboczej, który będzie integrował się z proponowanym rozwiązaniem (w ramach tej samej subskrypcji) w celu

zmiany hasła na stacji roboczej (gdy stacja zostanie podłączona do sieci lokalnej) i poinformowania narzędzia ochrony kont o realizacji zadania.

1.5 Oprogramowanie musi zapewniać wsparcie (możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego) dla systemów spoza listy "out of box" z wykorzystaniem skryptów lub innych mechanizmów realizowanych i wspieranych przez producenta rozwiązania w zakresie zmiany haseł poprzez: SSH / Telnet, API do zewnętrznych aplikacji, możliwość wykonywania zmian oraz weryfikacji spójności haseł poprzez symulację działań użytkownika w sesji aplikacji Web.

1.6 Oprogramowanie musi zapewniać możliwość automatycznego wykrywania kont w nowych urządzeniach Windows, usługach systemu Windows, zaplanowanych zadaniach, kontach serwisowych IIS itp., automatycznego dodania powyższych do produktu oraz automatycznie wymusić odpowiednią politykę zarządzania kontami uprzywilejowanymi.

1.7 Oprogramowanie musi posiadać możliwość ochrony (zarządzania) oraz dynamicznego generowania (w formie pseudolosowej) nowego klucza SSH zgodne z określonym szablonem.

1.8 Oprogramowanie musi automatycznie porównywać hasło/klucz SSH przechowywane w systemie oraz hasło/klucz SSH przechowywane na systemie docelowym.

1.9 Oprogramowanie musi automatycznie synchronizować hasło (oraz klucz SSH) przechowywane w systemie oraz hasło (oraz klucz SSH) przechowywane na systemie docelowym w przypadku wykrycia niezgodności.

1.10 Oprogramowanie musi umożliwiać przechowywanie historii rotacji haseł (np. trzy ostatnie hasła dla danego systemu docelowego) oraz umożliwiać łatwy dostęp do tej historii (np. poprzez interfejs webowy).

1.11 Oprogramowanie musi wspierać różne środowiska LDAP do uwierzytelniania użytkowników, nie mniej niż Sun One, MS Active-Directory, IBM Tivoli, Novel eDirectory, Oracle Internet Directory

1.12 Oprogramowanie musi umożliwiać wykrywanie par kluczy SSH w danej infrastrukturze.

1.13 Oprogramowanie musi umożliwiać zarządzanie i zapewniać bezpieczeństwo kluczy SSH używanych przez aplikacje w przypadku przechowywania kluczy w plikach konfiguracyjnych.

1.14 Producent musi udostępniać bezpłatnie dodatkową aplikację umożliwiającą automatyzację procesu tworzenia nowych skryptów do rotacji poświadczeń w systemach docelowych dostępnych z wykorzystaniem protokołu SSH. Aplikacja musi umożliwiać nagranie procesu ręcznego logowania użytkownika do systemu docelowego i rotacji poświadczeń, a następnie na podstawie nagrania musi automatycznie wygenerować skrypt / plugin który będzie wykorzystany przez silnik automatycznego zarządzania poświadczeniami konta.

Zarządzanie sesjami uprzywilejowanymi

1.15 Oprogramowanie musi umożliwiać zestawienie połączenia oraz monitoring sesji do systemu docelowego bez konieczności uprzedniego przekazania na stację użytkownika hasła konta uprzywilejowanego (po uwierzytelnieniu użytkownika oraz wskazaniu konta uprzywilejowanego produkt musi wprowadzić do dowolnie wybranej aplikacji dane dostępowe, dzięki czemu nie muszą być one udostępniane stacji użytkownika). Rozwiązanie musi udostępniać narzędzia do obsługi aplikacji instalowanych na systemie operacyjnym

modułu separacji oraz nagrywania sesji. Jako obsługa rozumiane jest uruchomienie aplikacji oraz wypełnienie pól danymi dostępowymi automatycznie pobranymi z zabezpieczonego, centralnego repozytorium kont uprzywilejowanych. W przypadku zestawienia połączeń przez przeglądarkę internetową narzędzie musi posiadać moduł umożliwiający realizację procesu utwardzania przeglądarki internetowej przez którą realizowana jest sesja uprzywilejowana (np. wyłączanie paska adresu, menu, narzędzi, widok theater mode, blokowanie wpisywania znaków podczas wypełniania danych dostępowych etc.).

1.16 Oprogramowanie musi umożliwiać zestawianie i zarządzanie sesjami uprzywilejowanymi do systemów chronionych, w szczególności (w sposób opisany w punkcie 1.15 niniejszego dokumentu, nie jest dopuszczalne zestawianie połączeń do poniższych systemów poprzez wykorzystanie dodatkowych modułów pośredniczących klasy jumphost / bastion host, do których użytkownik może się interaktywnie zalogować, wybrać aplikacje i ręcznie zestawić sesję do systemu chronionego):

a) posiadać wsparcie (dla monitoringu i separacji sesji oraz realizacji funkcji Single Systemach operacyjnych: Windows, Unix, Linux (Debian, Ubuntu, RedHat), pSeries (AIX),
b) Baz danych : Microsoft SQL, Oracle, MySQL, SAP HANA, DB2, PostgreSQL,
c) Systemów zarządzania infrastrukturą, aplikacji: DELL DRAC, RSA authentication Manager, HP iLO, SAP GUI, BMC Remedy,
d) Urządzeń sieciowych oraz systemów bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint (SmartDashboard, https, ssh), F5 Networks, FortiGate, Palo Alto Networks,
e) Narzędzi CI/CD (https, ssh): Chef, Jenkins, Kubernetes, Docker, Jfrog, GitHub,
f) Aplikacji typu SaaS/ stron web/ interfejsów web, minimum takich jak: Amazon Web Services (konsola zarządzania, IAM, integracja z STS), Zarządzanie Microsoft Azure
g) Środowisk wirtualizacyjnych VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh).

1.17 Sign-On dla kont uprzywilejowanych dla innych aplikacji oraz systemów niż wskazane w punkcie 1.16 poprzez możliwość wykorzystania nie mniej niż: uruchomienia aplikacji ze wskazanym zbiorem parametrów, zastosowania opisowego języka skryptowego, wbudowanego komponentu pozwalającego na obsługę własnych aplikacji web.

1.18 Producent musi udostępniać bezpłatnie dodatkową aplikację umożliwiającą automatyzację procesu tworzenia komponentów połączeniowych dla nowych / nieznanych aplikacji Web poprzez nagranie ręcznego połączenia użytkownika do aplikacji, automatyczną identyfikację nazw formularzy wykorzystywanych do wpisania poświadczeń przez użytkownika a następnie na podstawie nagrania automatyczne wygenerowanie odpowiedniego skryptu umożliwiającego połączenie zgodnie z opisem zawartym w punkcie 1.15 niniejszego dokumentu.

1.19 Oprogramowanie musi przechowywać nagrania sesji w zabezpieczonym kryptograficznie repozytorium uniemożliwiającym ich manipulację. Żaden z użytkowników włącznie z administratorem systemu nie może mieć wpływu na integralność składowanych nagrań (włącznie z brakiem możliwości ich usunięcia w zdefiniowanym okresie składowania danych).

1.20 Oprogramowanie musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie list dopuszczalnych i niedopuszczalnych poleceń wykonywanych poprzez SSH.

1.21 Oprogramowanie musi zapewniać rozliczalność w przypadku jednoczesnego wykorzystania konta współdzielonego przez więcej niż jednego użytkownika.

1.22 Oprogramowanie musi wykorzystywać mechanizmy indeksowania nagrań umożliwiające szybkie przeszukiwanie nagranych i monitorowanych sesji pod kątem występowania wskazanych słów kluczowych (wymagane są nie mniej niż następujące mechanizmy indeksowania: keystrokes, odpowiedzi okien systemu operacyjnego, komendy SQL). Nie jest dopuszczalnym dokonywanie indeksacji nagrań z wykorzystaniem mechanizmu OCR.

1.23 Oprogramowanie musi umożliwiać wykorzystanie przez moduł proxy opisany w punkcie 1.15 funkcjonalności Microsoft Remote App w celu publikowania aplikacji dostępowych. Skrypty utwardzające (and. Hardening) muszą być dostarczone przez Producenta rozwiązania oraz uruchomione podczas instalacji rozwiązania.

1.24 Oprogramowanie musi umożliwiać dostęp użytkowników do zasobu docelowego zgodnie z wymaganiami opisanymi w punkcie 1.15 przy wykorzystaniu nie mniej niż następujących metod / narzędzi:

a) interfejs Web proponowanego rozwiązania,

b) wykorzystanie różnych klientów RDP używanych na stacji, z której realizowany jest dostęp uprzywilejowany poprzez nie mniej niż: zdefiniowanie parametrów połączenia w ramach pliku konfiguracyjnego klienta RDP oraz możliwość interaktywnego odpytania użytkownika o właściwości systemu chronionego (takie jak adres, aplikacja kliencka, nazwa konta uprzywilejowanego) do którego będzie zestawione połączenie, przy czym wspierana musi metoda uwierzytelnienia do systemu bazująca na certyfikatach PKI,

c) wykorzystanie przeglądarki internetowej obsługującej html5 w celu zapewnienia wsparcia dla użytkowników korzystających z innych systemów operacyjnych niż Windows (brak klienta RDP na stacji użytkownika). W ramach połączenia realizowanego za pomocą tej metody sesja uprzywilejowana (zestawiona w oparciu o dowolną aplikację skonfigurowaną w systemie proxy, zgodnie z wymaganiami opisanymi w punkcie 1.15) musi być tunelowana w html5 i widoczna dla użytkownika jako nowa zakładka w przeglądarce,

d) Wykorzystanie różnych klientów linii poleceń i protokołu SSH (np. putty), przy czym wspierana musi metoda uwierzytelnienia do systemu bazująca na kluczach SSH.

1.25 Dla połączeń uprzywilejowanych zestawianych z poziomu interfejsu graficznego system/oprogramowanie musi umożliwiać wybór czy sesją ma być zestawiona ze stacji użytkownika w oparciu o protokół RDP czy protokół HTTPS (sesja tunelowana w html5 - mechanizm zestawiania sesji opisany w punkcie 1.24 podpunkt c),

1.26 Oprogramowanie musi wspierać tryb automatycznego, tymczasowego przypisywania konta użytkownika systemu Windows do grupy lokalnych administratorów po złożeniu stosownego wniosku (tzw. tryb dostępu Just-in-time / JIT). Nadane przez proponowany System uprawnienia JIT muszą być automatycznie odbierane po upływie czasu, na który został nadany dostęp.

1.27 Oprogramowanie musi wspierać tryb automatycznego generowania krótkoterminowych certyfikatów SSH w chronionych systemach Linux/Unix dla administratorów po złożeniu stosownego wniosku. Wygenerowane krótkoterminowe certyfikaty muszą być podpisane przez uprzednio utworzony klucz CA oraz zawierać klucz publiczny, informację o tożsamości wnioskującego administratora i opcjonalnie dodatkowe restrykcje przypisanego do wnioskującego.

1.28 Oprogramowanie musi umożliwiać transmisję plików oraz wykorzystanie schowka dla sesji tunelowanych w html5 (mechanizm zestawiania sesji opisany w punkcie 1.24 podpunkt c).

Zarządzanie incydentami bezpieczeństwa

1.29 Oprogramowanie musi posiadać funkcję kategoryzacji nagranych sesji użytkowników pod kątem ryzyka. Ryzyko opisane musi być poprzez konfigurację przez administratora systemu zbioru wykrywanych w trakcie trwania sesji funkcji / poleceń i przypisanej do nich wagi. Ryzyko musi być analizowane i przypisane zarówno dla zakończonych jak i aktywnych sesji. Informacje dotyczące poziomu ryzyka sesji muszą być widoczne zarówno w konsoli monitoringu sesji jak i w interfejsie obrazującym ryzyko / incydenty bezpieczeństwa (dashboard). Administrator musi posiadać możliwość określenia akcji wykonanych przez użytkownika dla których sesja powinna być automatycznie zakończona / wstrzymana.

1.30 Oprogramowanie musi posiadać wbudowane narzędzia analityczne umożliwiające automatyczne, bezobsługowe (bez konieczności definiowania reguł polityki bezpieczeństwa) wykrywanie podejrzanej aktywności kont uprzywilejowanych na bazie nauczonych automatycznie wzorców działania poszczególnych użytkowników (podejrzany czas pracy, nowy adres IP, zbyt duża ilość odwołań do repozytorium kont o hasła).

1.31 Oprogramowanie musi umożliwiać pobieranie danych o aktywnościach użytkowników z zewnętrznych systemów SIEM, wspierane muszą być nie mniej niż następujące rozwiązania: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee, FortiSIEM oraz zewnętrzne źródła informacji, minimum rsyslog (z systemów Unix/Linux), Windows Event Forwarder (z systemów Windows), AWS CloudTrail, Azure Function App.

1.32 Oprogramowanie musi umożliwiać podjęcie aktywnej akcji (co najmniej wymuszenie zmiany hasła konta uprzywilejowanego) w przypadku wykrycia anomalii wykorzystania kont uprzywilejowanych (nie mniej niż kradzież hasła konta uprzywilejowanego; utworzenie nowego konta i próba zestawienia nim połączenia z serwerem).

1.33 Oprogramowanie musi generować odpowiedni alarm w przypadku wykrycia nadmiernego wykorzystania kont uprzywilejowanych przez danego użytkownika oraz w przypadku wykorzystania konta uprzywilejowanego w niestandardowych godzinach (np. poza typowymi dla danego użytkownika godzinami pracy).

1.34 Oprogramowanie musi umożliwiać wykrywanie incydentów polegających na bezpośrednim dostępie użytkownika do systemu docelowego (np. bez wcześniejszego wysłania wniosku do proponowanego rozwiązania o hasło systemu docelowego) oraz na utworzeniu w systemie docelowym niezarządzanego do tej pory konta uprzywilejowanego. Rozwiązanie musi posiadać funkcje reagowania na tego typu działania poprzez wyegzekwowanie zmiany hasła konta uprzywilejowanego przez proponowany system, dodanie konta nowo utworzonego do centralnego repozytorium oraz automatyczny reset poświadczeń.

1.35 Oprogramowanie musi wykrywać i wysyłać powiadomienia (alarmy) o wykrytych podatności środowiska dotyczących kont uprzywilejowanych: nieszyfrowana komunikacja do systemu pozwalająca na przejęcie danych dostępowych kont uprzywilejowanych, użycie kont serwisowych w wielu celach (jako konta serwisowe i jednocześnie interaktywne), konta z włączoną funkcją "Unconstrained Delegation" oraz konta usług podatne na ataki klasy Kerberoasting (ang. risky SPNs).

1.36 Oprogramowanie musi umożliwiać wykrywanie nowych, niezarządzanych kont uprzywilejowanych oraz połączeń, które zostały nawiązane bez uprzedniego pobrania hasła z centralnego repozytorium, realizowanych w środowisku AWS i Azure.

1.37 Oprogramowanie musi umożliwiać monitoring, ingerencję oraz zakończenie aktywnej sesji graficznej w czasie jej trwania, a także określenie zbioru poleceń i uruchomionych funkcji systemu operacyjnego które spowodują automatyczne zakończenie / wstrzymanie sesji użytkownika (dla subskrypcji użytkownika wewnętrznego).

Architektura

1.38 Zaleca się, aby całość rozwiązania dostarczona Zamawiającemu była od tego/przez tego samego producenta, poszczególne moduły funkcjonalne muszą integrować się ze sobą.

1.39 Oprogramowanie musi umożliwiać zainstalowanie bazy danych z centralnym repozytorium poświadczeń na odseparowanym, utwardzonym systemie operacyjnym, który nie będzie współdzielony z pozostałymi modułami rozwiązania (jak proxy izolujące sesje, interfejs graficzny, moduł rotacji poświadczeń czy silnik analityczny).

1.40 Oprogramowanie musi posiadać budowę modularną, tzn. możliwość rozbudowy funkcjonalnej o kolejne komponenty, dostępne w ramach oddzielnych licencji/subskrypcji, odpowiedzialne za nie mniej niż:

- wieloskładnikowe uwierzytelnienie użytkowników (w tym przy wykorzystaniu kluczy sprzętowych) oraz zabezpieczenie dostępu do kluczowych aplikacji Web (wewnętrznych oraz chmurowych) poprzez moduł Single Sign-On (wymagania opisane w punkcie 2),
- ochronę dostępu zdalnego dla pracowników i zewnętrznych dostawców, wymagania opisane w punkcie 3,
- agentowe ograniczanie uprawnień użytkowników na stacjach Windows / MAC oraz serwerach Windows poprzez usuwanie kont lokalnych administratorów i podnoszenie uprawnień w kontekście konkretnych obiektów (skryptów, aplikacji, instalacji, dll i innych) dla konkretnych użytkowników, kontrolę aplikacyjną oraz blokowanie wycieku poświadczeń (np. haseł) z repozytoriów systemu operacyjnego Windows oraz aplikacji (np. przeglądarek internetowych, pamięci LSASS, SAM i innych),
- ochronę kont uprzywilejowanych w środowiskach DevOps,
- ochronę kont uprzywilejowanych zaszytych w kodzie statycznych aplikacji i skryptów,
- automatyczną klasyfikację ryzyka związanego ze zbyt obszernymi uprawnieniami w środowiskach chmurowych,
- automatyczne wykrywanie oraz reagowanie na ataki dotyczące kontrolerów domeny i protokołu kerberos (Overpass-the-hash, golden ticket, PAC manipulation, DCSync),

- agentowe ograniczanie dostępu do zbioru poleceń w połączeniach terminalowych do serwerów Linux/Unix (definiowanie centralnej polityki białych/czarnych list wykonywanych poleceń, podnoszenia uprawnień poprzez sudo, rozliczania użytkowników z wykonanych zadań).

1.41 Producent musi udostępniać procedury opisujące sposób utwardzania każdego z komponentów Systemu oraz dostarczone w paczkach instalacyjnych skrypty automatyzujące proces utwardzania dostosowane do każdego z modułów funkcyjnych. Utwardzanie każdego z komponentów musi być realizowane w oparciu o dobre praktyki producenta systemu operacyjnego oraz producenta rozwiązania PAM/PAS. Utwardzanie systemu operacyjnego modułu repozytorium poświadczeń musi być realizowane automatycznie przez instalator podczas procesu instalacji modułu.

1.42 Zaproponowane rozwiązanie/oprogramowanie musi uwzględniać nie mniej niż: jeden moduł składowania danych (poświadczeń, nagrań sesji etc), 5x moduł składowania danych na potrzeby Disaster Recovery/High Availability, 5x moduł do zmian i zarządzania kluczami oraz hasłami w systemach chronionych, 2 środowiska testowe pozwalające na odwzorowanie środowiska produkcyjnego.

1.43 Rozwiązanie/oprogramowanie nie może ograniczać liczby modułów odpowiedzialnych za izolację, monitoring oraz rejestrację sesji a także interfejsów Web, którymi użytkownik może podłączyć się do systemu ochrony kont uprzywilejowanych (dodanie kolejnych modułów nie może wymagać zakupu dodatkowych licencji/subskrypcji producenta systemu ochrony kont uprzywilejowanych).

1.44 Oprogramowanie musi wspierać rozproszoną architekturę, w której poszczególne moduły funkcyjne (proxy pośredniczące, moduły rotujące poświadczenia, interfejsy graficzne) zainstalowane są w wielu lokalizacjach (odseparowanych geograficznie) oraz komunikują się z elementami centralnymi (repozytorium poświadczeń) z wykorzystaniem bezpiecznego protokołu komunikacji zapewniającego bezpieczeństwo danych podczas transmisji, pracującego na jednym porcie TCP (do zadeklarowania podczas instalacji systemu). W przypadku infrastruktury rozproszonej całość systemu musi być zarządzana z centralnego interfejsu graficznego.

1.45 Zapewnienie wysokiej dostępności modułu składowania kont uprzywilejowanych musi być zaimplementowane na warstwie proponowanego oprogramowania (aplikacji), nie systemu operacyjnego/bazy danych, na którym oprogramowanie jest zainstalowane.

1.46 Produkt musi zapewniać ochronę kryptograficzną kopii zapasowych generowanych z produktu.

1.47 Rozwiązanie/oprogramowanie musi posiadać funkcję implementacji modułów składowania kont uprzywilejowanych w formie rozproszonej, złożonej z aktywnego modułu, redundancji modułu aktywnego oraz zbioru aktywnych modułów rozproszonych geograficznie, świadczących (w trybie odczytu) część funkcji użytkownikom (np. mechanizmy wykonywania kopii zapasowych, udostępniania danych kont uprzywilejowanych aplikacjom, dostęp do interfejsu użytkownika, możliwość zestawiania sesji uprzywilejowanych w sposób opisany w punkcie 1.15). Proponowane rozwiązanie/oprogramowanie musi obsługiwać nie mniej niż 6 aktywnych repozytoriów

poświadczeń. W przypadku infrastruktury rozproszonej całość systemu musi być zarządzana z centralnego interfejsu graficznego.

1.48 Rozwiązanie, w którym składowane są chronione konta uprzywilejowane musi uwzględniać zapasowe komponenty typu Disaster Recovery w lokalizacjach odseparowanych geograficznie. Musi istnieć możliwość wykorzystania trybu wysokiej dostępności (ang high availability) pomiędzy dwoma systemami współdzielącymi przestrzeń dyskową z zaszyfrowaną bazą danych oraz modułów zapasowych (ang. Disaster Recovery) w innych lokalizacjach (musi istnieć możliwość wdrożenia do 4 modułów Disaster Recovery w ramach podstawowej subskrypcji przy wdrożonym HA w lokalizacji podstawowej).

Integracje

1.49 Oprogramowanie musi umożliwiać integrację z systemami SIEM w celu wysyłania informacji o zarejestrowanych zdarzeniach w ramach monitorowanych sesji. Musi istnieć możliwość zdefiniowania typu zdarzeń, które powinny być wysłane do systemu SIEM.

1.50 Oprogramowanie musi wspierać integrację z rozwiązaniami typu HSM obsługującymi standard PKCS11, wymagana jest integracja z systemami: Atos HSM Proteccio, Gemalto Luna/Safenet 1700 Hardware Security Module, Thales nShield Hardware Security Module, Utimaco CryptoServer, Crypto4A QxEDGE, Fortanix SDKMS, i4p Trident, Unbound Key Control, Utimaco CryptoServer, HSM SafeNet ProtectServer External 2.

1.51 Oprogramowanie musi umożliwiać integrację z mechanizmami wykorzystywanymi do uwierzytelniania użytkowników, minimum hasła, LDAP, Windows NTLM, klucze SSH, Smart card, PKI, RADIUS, SAML, wieloskładnikowe uwierzytelnianie, RSA SecurID, Oracle SSO, Amazon Cognito Authentication, OpenID Connect (OIDC), klucze YubiKey 5.

Wymagania dodatkowe

1.52 Oprogramowanie musi posiadać skorelowaną ze sobą oficjalną metodykę implementacji, udostępnianą przez producenta systemu na stronie internetowej producenta. Metodyka ta musi zawierać minimum opis kroków, które należy wykonać w celu należytego i kompleksowego zaimplementowania rozwiązania typu PAS, umożliwiającego minimum ochronę dostępów uprzywilejowanych, wdrożenie polityki minimalnych uprawnień na stacjach roboczych i serwerach oraz ochronę kont uprzywilejowanych i danych uwierzytelniających wykorzystywanych przez aplikacje na potrzeby dostępu do innych systemów docelowych (włącznie z ochroną aplikacji wdrożonych w oparciu o metodykę DevOps). Metodyka poprzez analizę ryzyka musi umożliwiać pomoc w klasyfikacji kluczowych typów kont uprzywilejowanych oraz przypisanie ich do kolejnych etapów planowanej implementacji rozwiązania PAS. Metodyka musi być dostępna na oficjalnej stronie producenta na dzień składania ofert, link do oficjalnej strony producenta zawierającej opis metodyki należy dołączyć do oferty.

1.53 Proponowane oprogramowanie musi znajdować się w kwadracie "Leaders" raportu Gartner Magic Quadrant for Privileged Access Management za rok 2018, 2020 oraz 2021

2. Wieloskładnikowe uwierzytelnienie oraz zabezpieczenie dostępu do kluczowych aplikacji poprzez portal Single Sign-On

2.1 Oprogramowanie musi realizować funkcję:
   a) wieloskładnikowego adaptacyjnego uwierzytelnienia,
   b) zabezpieczenia dostępu zarówno do wewnętrznych jak i zewnętrznych (SaaS) aplikacji poprzez wykorzystanie zabezpieczonego portalu SSO,
   c) zarządzania cyklem życia tożsamości (ang. lifecycle management, wymagający dodatkowej subskrypcji).

2.2 Wymagana jest możliwość obsługi minimum następujących składników uwierzytelniających MFA: hasło, sms, email, oauth, aplikacja mobilna, phone call, pytanie bezpieczeństwa, Qrcode generowany w ramach procesu uwierzytelnienia do interfejsu Systemu, umożliwiający uwierzytelnienie użytkownika przy użyciu aplikacji mobilnej uprzednio zarejestrowanej w systemie, klucze sprzętowe YubiKey 5.

2.3 Oprogramowanie musi wspierać kontekstowe uwierzytelnianie bazujące na minimum następujących warunkach: adres IP, dzień tygodnia, data, zakres dat, zakres czasu, adaptacyjnie poprzez automatyczną analizę zachowań użytkowników (profilowanie urządzenia, adresu IP).

2.4 Moduł MFA poprzez protokół Radius musi umożliwiać integrację z popularnymi koncentratorami VPN jak minimum Cisco Systems, Palo Alto Networks, Pulse Secure, Fortinet.

2.5 Oprogramowanie musi być dostarczony jako usługa zewnętrzna (SaaS) wraz z modułem umożliwiającym integrację ze środowiskiem usług katalogowych AD/LDAP oraz uruchomienie serwera Radius dla klientów sieciowych Zamawiającego.

2.6 Oprogramowanie musi realizować usługę SSO dla aplikacji chmurowych oraz wewnętrznych, realizując w sposób scentralizowany bezpieczne uwierzytelnienie przy wykorzystaniu metod opisanych w punktach 2.02 oraz 2.03. Musi istnieć możliwość integracji z własnymi aplikacjami poprzez nie mniej niż następujące integracje:
   - plugin do przeglądarki,
   - NTLM,
   - Basic auth,
   - Klient Oauth2,
   - Serwer Oauth2,
   - OpenID Connect,
   - Saml,
   - WS-Fed,
   - Użytkownik – hasło.

2.7 Oprogramowanie musi posiadać gotowe integracje SSO z nie mniej niż następującymi aplikacjami: Adobe Sign, Amazon Web Services, Box, Dropbox, NetSuite, Office 365, Salesforce, ServiceNow, Slack, Webex, Zendesk.

3. Ochrona dostępu zdalnego

3.1 Rozwiązanie/oprogramowanie musi realizować funkcję bezpiecznego, uprzywilejowanego dostępu zdalnego dla pracowników firm zewnętrznych (zwanego dalej Dostępem

Zewnętrznym), bez konieczności instalacji rozwiązań klasy VPN (site-2-site lub client-site) po stronie sieci lub stacji roboczej firmy zewnętrznej.

3.2 Rozwiązanie/oprogramowanie nie może wymagać instalowania dodatkowego oprogramowania po stronie stacji roboczej użytkownika zewnętrznego poza przeglądarką internetową (wsparcie dla nie mniej niż przeglądarki Chrome, Edge, Firefox).

3.3 Proponowane rozwiązanie/oprogramowanie musi posiadać architekturę pozwalającą na zestawienie połączenia szyfrowanego pomiędzy stacją roboczą zewnętrznego dostawcy a siecią Zamawiającego bez konieczności otwierania ruchu przychodzącego do sieci Zamawiającego. W celu realizacji niniejszego punktu Rozwiązanie musi posiadać w swojej architekturze aplikację klasy SaaS (wymagane jest oferowanie przez Dostawcę aplikacji SaaS w rejonie Unii Europejskiej), do której z jednej strony zestawiany będzie ruch firm zewnętrznych, z drugiej zestawiane będzie bezpieczne połączenie z sieci Zamawiającego. Oprócz zwiększenia poziomu bezpieczeństwa Dostępu Zewnętrznego aplikacja musi realizować funkcję nadawania dostępu dla firm zewnętrznych, dzięki czemu Zamawiający będzie w stanie w trybie natychmiastowym (ang. Just-in-Time Provisioning) generować, akceptować i automatycznie wysyłać na podany podczas rejestracji adres e-mail wiadomości z zaproszeniem do zestawienia Dostępu Zewnętrznego. Aplikacja powinna umożliwiać zarządzanie utworzonymi użytkownikami (tworzenie nowych zaproszeń, nadawanie uprawnień, wyłączanie kont). Dostęp do aplikacji musi być możliwy poprzez wykorzystanie uwierzytelnienia biometrycznego, bez konieczności podawania danych dostępowych użytkownika (jak jego nazwa czy hasło).

3.4 Rozwiązanie/oprogramowanie musi obsługiwać uniwersalne uwierzytelnienie biometryczne (bez konieczności wpisywania przed zestawieniem połączenia danych dostępowych, jak użytkownik - hasło) realizowane przy użyciu stosowanych powszechnie urządzeń klasy smartphone.

3.5 Rozwiązanie/oprogramowanie musi posiadać wsparcie dla następujących platform mobilnych: IOS od wersji 10, Android od wersji 6.0. Dane biometryczne wykorzystywane do uwierzytelnienia składowane muszą być wyłącznie w modułach Secure Enclave / Trusted Execution Environment.

3.6 Oprócz realizacji funkcji uwierzytelnienia biometrycznego aplikacja mobilna oprogramowania musi posiadać funkcję potwierdzenia tożsamości dla kluczowych operacji realizowanych przez aplikację SaaS, np. nadawanie uprawnień administracyjnych innym użytkownikom.

3.7 W celu obsłużenia całości ruchu uprzywilejowanego do sieci Zamawiającego przez przeglądarkę internetową. Rozwiązanie/oprogramowanie musi posiadać wsparcie tunelowania sesji graficznych RDP przy użyciu HTML5 oraz protokołu SDP, zgodnie z wymaganiami punktu 1.24 podpunkt c niniejszego dokumentu.

3.8 Oprogramowanie musi wspierać transfer plików w trakcie trwania sesji graficznej

3.9 Oprogramowanie musi posiadać interfejs REST API do automatyzacji procesu zarządzania użytkownikami.

3.10 Oprogramowanie musi wspierać konfigurację dla wielu instytucji, zarówno od strony Zamawiającego jak i zewnętrznych dostawców (Zamawiający może zarządzać dostępami

wielu dostawców, dostawca potrzebuje wyłącznie jednej aplikacji na urządzeniu mobilnym by dostawać się do wielu Klientów, jeśli korzystają z tego samego rozwiązania)

3.11 Aplikacja mobilna oprogramowania musi posiadać funkcję zapraszania innych użytkowników. Proces ten musi umożliwiać automatyczne założenie tożsamości użytkownika zewnętrznego w systemie PAS.

4. Wdrożenie

4.1. PAM musi być uruchomiony w następującym zakresie:

1) PAM musi być zainstalowany w najnowszej wersji wraz z najnowszymi aktualizacjami.
2) Konfiguracja Oprogramowania PAM musi uwzględniać:
    a) Utworzenie kont użytkowników i grup w PAM zgodnie z wymaganiami Zamawiającego;
    b) Integrację uwierzytelniania i autoryzacji użytkowników PAM z usługą katalogową Active Directory wykorzystywaną przez Zamawiającego;
    c) Utworzenie kont systemów docelowych w PAM zgodnie z wymaganiami Zamawiającego;
    d) Utworzenie polityk związanych ze złożonością hasła zgodnie z wymaganiami Zamawiającego;
    e) Utworzenie harmonogramów zmiany hasła zgodnie z wymaganiami Zamawiającego;
    f) Utworzenie schematów wnioskowania o dostęp do hasła i/lub sesji zgodnie z wymaganiami Zamawiającego;
3) Dołączenie PAM do systemu monitoringu (Zabbix) Zamawiającego. Wykonawca określi kluczowe mierniki odnośnie wydajności i dostępności Oprogramowanie PAM oraz określi wartości progowe dla tych liczników, dzięki którym możliwe będzie proaktywne monitorowanie PAM. W szczególności określone zostaną przez Wykonawcę dopuszczalne wartości wskaźników wydajnościowych wszystkich składników systemu w warunkach normalnych oraz ich wartości progowe, których przekroczenie będzie uznawane za sytuację alarmową i sytuację krytyczną.
4) Wykonanie testów akceptacyjnych:
    a) Uruchamianie i zatrzymywanie rozwiązania PAM;
    b) Weryfikacja procesu zarzadzania hasłami na kontach systemów docelowych;
    c) Weryfikacja procesu zarzadzania sesjami;
    d) Weryfikacja poprawności działania procedur;

5. Instruktaż

5.1. Zamawiający wymaga od Wykonawcy przeprowadzenia instruktażu dla 5 administratorów oprogramowania PAM.

5.2. Instruktaż odbędzie się w siedzibie Zamawiającego w uzgodnionym na roboczo pomiędzy Wykonawcą a Zamawiającym terminie. W przypadku gdy nie będzie możliwości zorganizowania instruktażu w siedzibie Zamawiającego, dopuszcza się zorganizowanie instruktażu w formie zdalnej.

5.3. Zamawiający wymaga, aby instruktaż składał się z części teoretycznej i warsztatowej, i trwał minimum 16 godzin (min. 2 dni robocze).

5.4. Zapewnienie infrastruktury dla części warsztatowej leży po stronie Wykonawcy.

5.5. Zakres szkolenia:

1) Ogólna architektura Oprogramowania PAM;
2) Bezpieczeństwo Oprogramowania PAM;
3) Konfiguracja kont systemów docelowych w Oprogramowaniu PAM;
4) Zarządzanie użytkownikami w Oprogramowaniu PAM i integracja z innymi mechanizmami uwierzytelnienia i autoryzacji;
5) Polityki złożoności hasła, harmonogram zmian haseł, walidacja poprawności zmiany hasła;
6) Zarządzanie sesjami w Oprogramowaniu PAM;
7) Zarządzanie schematami wnioskowania i akceptacji dostępu hasła i/lub sesji w Systemie PAM;
8) Audyt i raportowanie w Oprogramowaniu PAM;
9) Procedura aktualizacji Oprogramowania PAM;
10) Rozwiązywanie problemów;

6. Gwarancja i wsparcie techniczne

6.1. Oprogramowanie PAM powinien być objęty 12 miesięczną gwarancja i wsparciem technicznym producenta oraz Wykonawcy.

6.2. Usługi w ramach gwarancji, w tym usuwanie Awarii, będą realizowane zgodnie z następującymi zasadami i terminami:

1) czas reakcji – nie później niż w ciągu 1 godziny od momentu zgłoszenia wady oprogramowania PAM lub Awarii w sposób wskazany w §4 ust.3 Umowy do momentu potwierdzenia przyjęcia tego zgłoszenia, przesłanego na adres poczty elektronicznej Zamawiającego;
2) czas usunięcia wady Oprogramowania PAM lub Awarii – nie później niż w ciągu 24 godzin od momentu zgłoszenia wady Oprogramowania PAM lub Awarii w sposób wskazany w §4 ust.3 Umowy do momentu potwierdzenia jej usunięcia przesłanego na adres poczty elektronicznej Zamawiającego. Jeśli po weryfikacji Zamawiający uzna, że dana wada Oprogramowania PAM lub Awaria nie została usunięta, to przysługuje mu prawo do zgłoszenia tego faktu w nowym zgłoszeniu wady Oprogramowania PAM lub Awarii, przy czym czas jej trwania liczy się jako kontynuacja pierwotnie zgłoszonej i nie usuniętej należycie wady lub Awarii;
3) w przypadku braku możliwości usunięcia wady lub Awarii w ciągu 24 godzin od momentu zgłoszenia, Zamawiający dopuszcza zastosowanie czasowego obejścia rozwiązania problemu w uzgodnieniu i za akceptacją Zamawiającego, jednak docelowe

rozwiązanie problemu musi zostać dostarczone i zaimplementowane w czasie 30 dni liczonych od dnia następnego po dniu wdrożenia tymczasowego obejścia problemu.

6.3. Zakres usług wsparcia technicznego obejmuje:

1) doradztwo i pomoc w zakresie obsługi Oprogramowania PAM;
2) analizę i rozwiązywanie problemów związanych z Oprogramowania PAM oraz zaistniałych na styku pomiędzy Oprogramowaniem PAM i/lub Sprzętem Teleinformatycznym i innym oprogramowaniem użytkowanym przez Zamawiającego;
3) zapewnienie dostępu (za pośrednictwem strony internetowej) i możliwości korzystania z aktualizacji, poprawek Oprogramowania PAM, nowych wersji oprogramowania, oraz dokumentacji administracyjnej i technicznej dotyczącej oprogramowania PAM;
4) informowanie o znanych problemach z Oprogramowania PAM i sposobach ich rozwiązania drogą telefoniczną - lub poprzez pocztę elektroniczną.

6.4. W sytuacji, gdy pomoc Wykonawcy realizowana w ramach wsparcia technicznego, o którym mowa w ust. 6.2 i 6.3, okaże się niewystarczająca dla Zamawiającego, Wykonawca zobowiązuje do świadczenia na wniosek Zamawiającego dodatkowych usług wsparcia merytorycznego w wymiarze 160 godzin przez okres 12 miesięcy, polegających na osobistym (bezpośrednim) wsparciu Zamawiającego w miejscu instalacji Oprogramowania PAM bądź w formie zdalnej przez wykwalifikowanych polskojęzycznych inżynierów w pełnym zakresie, w tym:

1) usuwaniu Awarii na zasadach wskazanych OPZ oraz Umowie.
2) aktualizacji wersji wszystkich komponentów Oprogramowania PAM oraz przeprowadzania odpowiednich testów poprawnego funkcjonowania Oprogramowania PAM po ww. aktualizacjach;
3) wdrażania nowych funkcjonalności Oprogramowania PAM, wynikających z ww. aktualizacji;
4) pełnej instalacji i konfiguracji Oprogramowania PAM;
5) oraz innych prac serwisowych dotyczących Oprogramowania PAM, na życzenie Zamawiającego.

Znak sprawy: BA.WZP.26.44.2022

Załącznik nr 2 do SWZ

Formularz oferty	
Nazwa Wykonawcy[1]:	Kliknij tutaj, aby wprowadzić tekst.
Adres:	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Wybierz element.
REGON lub NIP[2]:	Kliknij tutaj, aby wprowadzić tekst.
PESEL lub KRS:	Kliknij tutaj, aby wprowadzić tekst.
Numer telefonu Wykonawcy wraz z numerem kierunkowym:	Kliknij tutaj, aby wprowadzić tekst.
Adres e-mail Wykonawcy:	Kliknij tutaj, aby wprowadzić tekst.
Wykonawca jest:[3]	☐ mikroprzedsiębiorstwem ☐ małym przedsiębiorstwem ☐ średnim przedsiębiorstwem ☐ jednoosobowa działalność gospodarcza ☐ osoba fizyczna nieprowadząca działalności gospodarczej ☐ inny rodzaj …….
Nr konta bankowego, na które będzie kierowane wynagrodzenie dla Wykonawcy, w przypadku podpisania umowy	…… Wykonawca zobowiązany jest do podania numeru rachunku bankowego, który widnieje w Wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT, prowadzonym przez Ministerstwo Finansów (jeżeli dotyczy)
Adres Wykonawcy, z którego przesyłane będą faktury elektroniczne	……

[1] W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia – należy podać wszystkie dane Lidera, a w odniesieniu do pozostałych wykonawców należy podać tylko nazwę i krajowy numer identyfikacyjny (REGON lub NIP).

[2] W przypadku polskich wykonawców należy podać numer REGON lub NIP.

[3] Por. zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz. U. L. 124 z 20.5.2003, s. 36) Te informacje są wymagane wyłącznie do celów statystycznych.
Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub suma bilansowa nie przekracza 10 milionów Euro.
Średnie przedsiębiorstwa: przedsiębiorstwa, które nie SA mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów Euro lub roczna suma bilansowa nie przekracza 43 milionów Euro.

Przystępując do prowadzonego postępowania o udzielenie zamówienia publicznego na:

„Uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze Zamawiającego”

oferuję/oferujemy realizację zamówienia, zgodnie ze specyfikacją warunków zamówienia**:**

za następującą cenę (cenę oferty – **maksymalne wynagrodzenie**):

Kliknij tutaj, aby wprowadzić tekst. zł netto,

stawka VAT Kliknij tutaj, aby wprowadzić tekst.%, tj. Kliknij tutaj, aby wprowadzić tekst. zł,

Kliknij tutaj, aby wprowadzić tekst. zł brutto,

w tym:

- **koszt z tytułu wykonania analizy środowiska i sporządzenia projektu technicznego:**

  Kliknij tutaj, aby wprowadzić tekst. zł netto,

  stawka VAT Kliknij tutaj, aby wprowadzić tekst.%, tj. Kliknij tutaj, aby wprowadzić tekst. zł,

  Kliknij tutaj, aby wprowadzić tekst. zł brutto,

- **koszt z tytułu uruchomienia i konfiguracji rozwiązania PAM (Privileged Access Management)”:**

  Kliknij tutaj, aby wprowadzić tekst. zł netto,

  stawka VAT Kliknij tutaj, aby wprowadzić tekst.%, tj. Kliknij tutaj, aby wprowadzić tekst. zł,

  Kliknij tutaj, aby wprowadzić tekst. zł brutto,

- **koszt z tytułu udzielenia/zapewnienia licencji/subskrypcji rozwiązania PAM (Privileged Access Management):**

  Kliknij tutaj, aby wprowadzić tekst. zł netto,

  stawka VAT Kliknij tutaj, aby wprowadzić tekst.%, tj. Kliknij tutaj, aby wprowadzić tekst. zł,

  Kliknij tutaj, aby wprowadzić tekst. zł brutto,

- **koszt z tytułu przeprowadzenia instruktażu z uruchomienia, konfiguracji i administracji PAM (Privileged Access Management):**

  Kliknij tutaj, aby wprowadzić tekst. zł netto,

  stawka VAT Kliknij tutaj, aby wprowadzić tekst.%, tj. Kliknij tutaj, aby wprowadzić tekst. zł,

  Kliknij tutaj, aby wprowadzić tekst. zł brutto,

- **koszt z tytułu wykonania sporządzenia i dostarczenia dokumentacji powdrożeniowej:**

  Kliknij tutaj, aby wprowadzić tekst. zł netto,

  stawka VAT Kliknij tutaj, aby wprowadzić tekst.%, tj. Kliknij tutaj, aby wprowadzić tekst. zł,

  Kliknij tutaj, aby wprowadzić tekst. zł brutto,

- **koszt z tytułu świadczenia realizacji usługi merytorycznego wsparcia administratorów rozwiązania PAM (Privileged Access Management) w ilości 160 godzin w okresie 12 miesięcy:**

  - **KOSZT ZA 160 ROBOCZOGODZIN:**

  Kliknij tutaj, aby wprowadzić tekst. zł netto,

  stawka VAT Kliknij tutaj, aby wprowadzić tekst.%, tj. Kliknij tutaj, aby wprowadzić tekst. zł,

  Kliknij tutaj, aby wprowadzić tekst. zł brutto,

- **STAWKA ZA 1 ROBOCZOGODZINĘ:**

Kliknij tutaj, aby wprowadzić tekst. zł netto,

stawka VAT Kliknij tutaj, aby wprowadzić tekst.%, tj. Kliknij tutaj, aby wprowadzić tekst. zł, Kliknij tutaj, aby wprowadzić tekst. zł brutto,

Oferujemy następujący czas reakcji na zgłoszenie w ramach merytorycznego wsparcia administratorów (zaznaczyć odpowiednio):

☐ powyżej 48 h

☐ powyżej 24 h i nie więcej niż 48 h

☐ do 24 h

Jako osobę pełniącą nadzór nad realizacją umowy (pełniąca funkcję Koordynatora odpowiedzialnego za prawidłową realizację zamówienia), zatrudnioną na podstawie umowy o pracę przez cały okres trwania umowy wskazujemy:

Lp.	Dane Koordynatora	Podstawa do dysponowania osobą
1	…… (imię i nazwisko, nr tel., adres e-mail)	

Jednocześnie oświadczam, że:

1) zapoznałem się z treścią SWZ, wyjaśnieniami do SWZ oraz modyfikacjami SWZ i nie wnoszę do niej żadnych zastrzeżeń. Tym samym zobowiązuję się do spełnienia wszystkich warunków zawartych w SWZ;
2) akceptuję postanowienia umowne zawarte w załączonym do SWZ projekcie Umowy i w przypadku wybrania mojej oferty jako najkorzystniejszej, zobowiązuję/my się do podpisania umowy na warunkach zawartych w SWZ oraz w miejscu i terminie wyznaczonym przez Zamawiającego;
3) Oświadczam, że jestem związany ofertą w terminie wskazanym w SWZ.
4) Oświadczam, że przedmiot zamówienia wykonam*:

   ☐ siłami własnymi, tj. bez udziału podwykonawców;

   ☐ przy udziale podwykonawców:

L.p.	Część zamówienia, którą Wykonawca zamierza powierzyć do wykonania podwykonawcom	Nazwy podwykonawców
1.	Kliknij tutaj, aby wprowadzić tekst. - Wybierz element. niż 10% wartości zamówienia**	Kliknij tutaj, aby wprowadzić tekst.
2.	Kliknij tutaj, aby wprowadzić tekst. - Wybierz element. niż 10% wartości zamówienia**	Kliknij tutaj, aby wprowadzić tekst.
3.	Kliknij tutaj, aby wprowadzić tekst. - Wybierz element. niż 10% wartości zamówienia**	Kliknij tutaj, aby wprowadzić tekst.

*) Proszę zaznaczyć odpowiednie pole wyboru.

Uwaga: brak wpisu i skreślenia powyżej rozumiany jest, iż przedmiotowe zamówienie realizowane będzie bez udziału podwykonawców.

5) TAJEMNICA PRZEDSIĘBIORSTWA:

Oświadczam, że (zaznaczyć odpowiednio):

☐ oferta nie zawiera tajemnicy przedsiębiorstwa;

☐ pliki o nazwach …… stanowią tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), co zostało wykazane w treści oświadczenia zamieszczonego w pliku o nazwie ……

6) Zgodnie z treścią art. 225 ust. 2 ustawy Pzp informuję, że***:

☐ wybór niniejszej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2021 r., poz. 685 z późn. zm.):

☐ wybór niniejszej oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2021 r., poz. 685 z późn. zm.), oraz:

a) wskazuję nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego:

Kliknij tutaj, aby wprowadzić tekst.,

b) wskazuję wartość towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku: Kliknij tutaj, aby wprowadzić tekst.,

c) wskazuję stawkę podatku od towaru i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie: Kliknij tutaj, aby wprowadzić tekst.%.

***) Proszę zaznaczyć odpowiednie pole wyboru. Uwaga – niewskazanie żadnej z ww. treści oświadczenia i niewypełnienie powyższych danych – Zamawiający uzna, że wybór przedmiotowej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.

7) Oświadczam, że****:

☐ wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO (rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE - ogólne rozporządzenie o ochronie danych; Dz. Urz. UE L 119 z 04.05.2016, str. 1), wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.****

☐ nie wypełniłem ww. obowiązków informacyjnych

****) W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa.

8) Osoba działająca w imieniu Wykonawcy jest umocowana do Jego reprezentowania na podstawie*****

a) wpisu do:

☐ Krajowego Rejestru Sądowego,

☐ Centralnej Ewidencji i Informacji o Działalności Gospodarczej,

☐ innego rejestru – jeżeli tak, należy wskazać właściwy: Kliknij tutaj, aby wprowadzić tekst.

b) innego dokumentu:

☐ pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania Wykonawcy w przypadku, gdy prawo to nie wynika z ww. ogólnodostępnych dokumentów.

Osoba uprawniona do kontaktów z Zamawiającym:

Kliknij tutaj, aby wprowadzić tekst.

tel. Kliknij tutaj, aby wprowadzić tekst.

e-mail Kliknij tutaj, aby wprowadzić tekst.

***) Proszę zaznaczyć odpowiednie pole wyboru oraz podać dane osoby uprawnionej do kontaktu

Do niniejszej oferty załączam[4]:

1) ☐ pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania Wykonawcy (o ile prawo to nie wynika z ogólnodostępnych dokumentów (w bazie KRS lub CEiDG));
2) ☐ pełnomocnictwo do reprezentowania Wykonawcy lub Wykonawców wspólnie ubiegających się o udzielenie zamówienia (jeżeli dotyczy);
3) ☐ oświadczenie, z którego wynika, które usługi wykonają poszczególni Wykonawcy (jeżeli dotyczy);
4) ☐ oświadczenie o nie podleganiu wykluczeniu;
5) ☐ oświadczenie na potwierdzenie braku podstaw wykluczenia z art. 7 ust. 1 ustawy sankcyjnej.
6) Kliknij tutaj, aby wprowadzić tekst.

Podpisy osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy

……..

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym

[4] Zaznaczyć odpowiednio

Znak sprawy: BA.WZP.26.44.2022

Załącznik nr 3 do SWZ

Oświadczenie dotyczące braku podstaw wykluczenia z postępowania, nr sprawy BA.WZP.26.44.2022

Oświadczam, co następuje:

DANE WYKONAWCY / PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY / PODWYKONAWCY* *niepotrzebne skreślić	
pełna nazwa/firma	
Adres	
NIP/PESEL w zależności od podmiotu	
KRS/CEiDG w zależności od podmiotu	
adres strony, z której można pobrać ww. dokumenty	
Osoba reprezentująca, podstawa do reprezentacji	
OŚWIADCZENIA DOTYCZĄCE WYKONAWCY / PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY:	
~~Czy Wykonawca / podmiot udostępniający zasoby oświadcza, że spełnia warunki udziału w postępowaniu określone przez Zamawiającego w Rozdziale 9 SWZ~~ ~~[…..] TAK […..] NIE~~	
Czy Wykonawca / ~~podmiot udostępniający zasoby~~ podlega wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp. […..] TAK […..] NIE	
Czy Wykonawca / ~~podmiot udostępniający zasoby~~ podlega wykluczeniu z postępowania na podstawie art. 109 ust. 1 pkt 1, 4, 5, 7 ustawy Pzp. […..] TAK […..] NIE	
Zachodzą w stosunku do Wykonawcy / ~~podmiotu udostępniającego zasoby~~ podstawy wykluczenia z postępowania na podstawie art. ……. Ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 lub art. 109 ust. 1 pkt 1, 4, 5, 7 ustawy Pzp).	
W związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp zostały podjęte następujące środki naprawcze: …….	
OŚWIADCZENIE WYPEŁNIANE PRZEZ PODWYKONAWCĘ NIEBĘDĄCEGO PODMIOTEM, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:	
Czy podwykonawca podlega wykluczeniu z postępowania na podstawie art. 108 ust. 1 lub art. 109 ust. 1 pkt 1, 4, 5, 7 ustawy Pzp. […..] TAK […..] NIE	
OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI: Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.	

UWAGA:

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym.

W przypadku składania oferty przez wykonawców występujących wspólnie, powyższe oświadczenie składa każdy wykonawca (np. członek konsorcjum, wspólnik w spółce cywilnej) o ile ma zastosowanie.

W przypadku polegania na zdolnościach podmiotu udostępniającego zasoby powyższe oświadczenie składa także podmiot udostępniający zasób o ile ma zastosowanie.

Znak sprawy: BA.WZP.26.44.2022

Załącznik nr 4 do SWZ

Oświadczenie o przynależności albo braku przynależności do tej samej grupy kapitałowej, nr sprawy BA.WZP.26.44.2022

Dotyczy postępowania o udzielenie zamówienia publicznego pn.: „**Uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze Zamawiającego”** w imieniu Wykonawcy:

.....
(Nazwa Wykonawcy)

oświadczam, że:

***) nie należę** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r., poz. 275) z innym Wykonawcą, który złożył odrębną ofertę w przedmiotowym postępowaniu o udzielenie zamówienia publicznego;

***) należę** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r., poz. 275) z innym Wykonawcą, , niżej wskazanym, który złożył odrębną ofertę w przedmiotowym postępowaniu o udzielenie zamówienia publicznego:

1) Kliknij tutaj, aby wprowadzić tekst.
2) Kliknij tutaj, aby wprowadzić tekst.

Jednocześnie przedkładam następujące dokumenty lub informacje potwierdzające przygotowanie oferty niezależnie od ww. Wykonawcy[5]:

1) Kliknij tutaj, aby wprowadzić tekst.
2) Kliknij tutaj, aby wprowadzić tekst.

Podpisy osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy

.....

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym.

*Niepotrzebne skreślić

[5] Wraz z oświadczeniem o przynależności do grupy kapitałowej z innym Wykonawcą, który złożył odrębną ofertę lub ofertę częściową w przedmiotowym postępowaniu o udzielenie zamówienia publicznego, Wykonawca załącza dokumenty bądź informacje potwierdzające, że powiązania z tym Wykonawcą nie prowadzą do zakłócenia konkurencji

Znak sprawy: BA.WZP.26.44.2022

Załącznik nr 5 do SWZ

Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia, o którym mowa w art. 117 ust. 4 ustawy Pzp, nr sprawy BA.WZP.26.44.2022

W imieniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia pn. „**Uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze Zamawiającego”**, oświadczam, iż przedmiot zamówienia wykonamy zgodnie z następującym podziałem czynności:

Lp.	Nazwa/imię i nazwisko Wykonawcy	Zakres czynności
1.	*Wykonawca nr 1*	
2.	*Wykonawca nr 2*	

Podpisy osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy

……..

***Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym*.**

Znak sprawy: BA.WZP.26.44.2022

Załącznik nr 6 do SWZ

Projekt umowy

UMOWA Nr ……

zawarta pomiędzy:

Skarbem Państwa - Urzędem Komunikacji Elektronicznej z siedzibą w Warszawie (01-211), ul. Giełdowa 7/9, NIP 527-23-67-496, zwanym dalej **„Zamawiającym”**, reprezentowanym przez:

……. – ……

a

…… z siedzibą w …… (…-...) przy ul. ……., wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez …….. w ……., …….. Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem: ……., REGON: ……., NIP: ……., wysokość kapitału zakładowego: ……. PLN, zwaną „**Wykonawcą”**, reprezentowaną przez:

……..

zwanymi także łącznie **„Stronami”**,
o następującej treści:

§ 1

Umowa zawarta została w wyniku postępowania o udzielenie zamówienia publicznego w trybie podstawowym - art. 275 pkt.1 – numer sprawy BA.WZP.26.44.2022. ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2022 r. poz. 1710 z późn. zm.) zwanej dalej „ustawą Pzp” – w wyniku którego za najkorzystniejszą uznano ofertę Wykonawcy.

§ 2
Przedmiot Umowy

1. Przedmiotem Umowy jest uruchomienie licencji rozwiązania Privilege Access Management (dalej: PAM) w infrastrukturze Zamawiającego (producent: ……., typ/model: ……..), które obejmuje w szczególności:
    7) wykonanie Analizy środowiska Zamawiającego oraz sporządzenie Projektu Technicznego;
    8) uruchomienie i konfiguracja rozwiązania PAM w najnowszej dostępnej wersji;
    9) udzielenie lub zapewnienie udzielenia licencji/subskrypcji dla oprogramowania PAM na warunkach producenta wraz z gwarancją i usługą wsparcia technicznego na okres 12 miesięcy, w tym:

a. możliwość pracy 20 administratorów będących pracownikami Zamawiającego oraz
b. możliwość pracy 50 kontraktorów (zewnętrznych dostawców)

10) przeprowadzenie instruktażu dla Zamawiającego z uruchomienia, konfiguracji i administracji PAM;
11) sporządzenie i dostarczenie Zamawiającemu Dokumentacji Powykonawczej;
12) merytoryczne wsparcie administratorów rozwiązania PAM w ilości 160 godzin w okresie 12 miesięcy.

2. Szczegółowo Przedmiot Umowy został określony w Załączniku nr 1 do Umowy.
3. Wykonawca oświadcza, że posiada odpowiedni potencjał techniczny, kadrowy i ekonomiczny oraz posiada wymaganą przez Zamawiającego autoryzację producentów oprogramowania, niezbędną do wypełnienia postanowień Umowy.

§ 3
Terminy i sposób realizacji

1. Przedmiot umowy, o którym mowa w § 2 ust. 1, zostanie zrealizowany przez Wykonawcę w następujących terminach:
   1) wykonanie Analizy środowiska Zamawiającego oraz sporządzenie Projektu Technicznego w terminie max. 7 dni od podpisania Umowy.
   2) uruchomienie i konfiguracja PAM w środowisku Zamawiającego w terminie do 20.12.2022;
   3) przeprowadzenie instruktażu dla Zamawiającego z uruchomienia, konfiguracji i administracji PAM w terminie do 20.12.2022;
   4) sporządzenie i dostarczenie Zamawiającemu Dokumentacji Powykonawczej w terminie do 20.12.2022;
   5) świadczenie merytorycznego wsparcie administratorów rozwiązania PAM w ilości 160 godzin w okresie 12 miesięcy, licząc od dnia podpisania Końcowego Protokołu Odbioru.
2. Wykonawca dostarczy Zamawiającemu dokument wystawiony przez Producenta/dystrybutora potwierdzający zapewnienie Zamawiającemu prawa do licencji/subskrypcji oraz gwarancji i usługi wsparcia technicznego w terminie do 20.12.2022.

§ 4
Komunikacja między Stronami

1. Ze strony Zamawiającego osobą upoważnioną do kontaktów z Wykonawcą w sprawach dotyczących realizacji Umowy oraz do podpisania protokołu odbioru jest **……**, tel. ……., e-mail: …….. lub ……., tel. ……., e-mail: …….
2. Do kontaktów z Zamawiającym podczas realizacji Umowy (Koordynator odpowiedzialny za prawidłową realizację zamówienia) oraz podpisania protokołu odbioru ze strony Wykonawcy wyznaczony jest **……**, tel. ……., e-mail: ……
3. Zgłoszenie w ramach gwarancji, w tym zgłoszenie konieczności usunięcia Awarii, będzie dokonywane bezpośrednio Wykonawcy telefonicznie – pod polskim numerem telefonicznym ……. lub na adres poczty elektronicznej …….. . Zgłoszenia przyjmowane będą w dni robocze w godz. 8-16.

4. Zmiana osób, o których mowa w ust. 1-2 nie wymaga zmiany Umowy. Zmiana następuje poprzez pisemne oświadczenie złożone drugiej Stronie o dokonaniu zmiany i wskazaniu osoby lub osób do wykonywania czynności określonych w niniejszym paragrafie.

§ 5
Odbiór

1. Wykonanie przedmiotu Umowy o którym mowa w § 2 ust. 1 Umowy zostanie potwierdzone podpisaniem protokołu odbioru, sporządzonym przez Wykonawcę w porozumieniu z Zamawiającym.
2. Wzór protokołu odbioru stanowi Załącznik nr 2 do Umowy.

§ 6
Wynagrodzenie

1. Wynagrodzenie (maksymalna kwota) za prawidłową realizację Przedmiotu Umowy Strony ustaliły na kwotę netto: **…….. zł** (słownie:……), co stanowi kwotę brutto w wysokości: **…….. zł** (słownie: ……), na które składa się:
    a) Kwota brutto: …….. zł – z tytułu wykonania analizy środowiska i sporządzenia projektu technicznego;
    b) Kwota brutto: …….. zł – z tytułu uruchomienia i konfiguracji rozwiązania PAM;
    c) Kwota brutto: …….. zł – z tytułu udzielenia/zapewnienia licencji/subskrypcji rozwiązania PAM na warunkach producenta wraz z gwarancją;
    d) Kwota brutto: …….. zł – z tytułu przeprowadzenia instruktażu z uruchomienia, konfiguracji i administracji PAM;
    e) Kwota brutto: …….. zł – z tytułu sporządzenia i dostarczenia dokumentacji powdrożeniowej;
    f) Kwota brutto: …….. zł – z tytułu realizacji usługi merytorycznego wsparcia administratorów rozwiązania PAM w ilości 160 godzin w okresie 12 miesięcy.
2. Kwota wymieniona w ust. 1 obejmuje wszystkie koszty jakie poniesie Wykonawca z tytułu należytej i zgodnej z Umową oraz obowiązującymi przepisami realizacji Przedmiotu Umowy.
3. Wynagrodzenie za 1 roboczogodzinę wsparcia administratorów rozwiązania PAM, o którym mowa w ust. 1 lit. f) ustalono na kwotę brutto w wysokości: ….. zł (słownie: …….).
4. Płatność wynagrodzenia, o którym mowa w ust. 1 niniejszego paragrafu nastąpi jednorazowo po uruchomieniu, co zostanie potwierdzone protokołem odbioru.
5. Zapłata, o której mowa w ust. 1 nastąpi przelewem na rachunek bankowy Wykonawcy nr ……., w terminie 21 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT wraz z podpisanym przez Zamawiającego protokołem odbioru.
6. Zmiana rachunku bankowego Wykonawcy, o którym mowa w ust. 4, nie wymaga zawarcia aneksu do Umowy. Zmiana następuje na podstawie złożonego przez Wykonawcę oświadczenia o zmianie i wskazaniu nowego numeru rachunku bankowego. Oświadczenie musi zostać podpisane przez osobę/ osoby upoważnione do reprezentowania Wykonawcy i doręczone w formie pisemnej do siedziby Zamawiającego.
7. Fakturę należy wystawić i dostarczyć w formie pisemnej lub elektronicznej. W przypadku faktury pisemnej na adres: Urząd Komunikacji Elektronicznej, ul. Giełdowa 7/9, 01-211 Warszawa, natomiast w przypadku faktury elektronicznej z adresu Wykonawcy: …… na adres Zamawiającego: sekretariat.bi@uke.gov.pl
8. W przypadku dostarczenia przez Wykonawcę faktury w formie elektronicznej na inny adres e-mail lub z innego adresu e-mail niż wskazany powyżej w ust. 6 taką fakturę uznaje się za niedostarczoną.

9. Na fakturze należy umieścić numer identyfikacji podatkowej Zamawiającego: 527-23-67-496 oraz informację, że Przedmiot Umowy realizowany jest na podstawie Umowy wraz ze wskazaniem jej numeru.
10. Zamawiający może wstrzymać zapłatę faktury VAT wystawionej niezgodnie obowiązującymi przepisami lub Umową, do czasu otrzymania faktury korygującej lub odpowiednio do momentu ziszczenia się wszystkich warunków określonych w treści Umowy, których spełnienie jest wymagane przed wystawieniem danej faktury.
11. Wynagrodzenie Wykonawcy, o którym mowa w ust. 1 lit. f) niniejszego paragrafu zostanie odpowiednio zmienione (zmniejszone lub zwiększone) w wysokości wynikającej ze wskaźnika wzrostu (spadku) cen towarów i usług konsumpcyjnych publikowanego przez Główny Urząd Statystyczny – dalej jako: „wskaźnik GUS" – za poprzedni rok kalendarzowy.
12. Minimalny poziom zmiany wskaźnika GUS, w wyniku którego wynagrodzenie Wykonawcy zostanie zmienione wynosi 2%, w stosunku do wskaźnika wzrostu (spadku) cen towarów i usług konsumpcyjnych (poziom zmiany ceny) publikowanego przez Główny Urząd Statystyczny.
13. Wykonawca zobowiązany jest do wykazania wpływu zmiany wskaźnika GUS na wykonanie przedmiotu Umowy. Wykazanie wpływu następuje w formie pisemnej. Wykonawca składa wyczerpujące uzasadnienie faktyczne i prawne oraz dokładne wyliczenie kwoty cen materiałów i kosztów przed i po zmianie wynagrodzenia.
14. Strony nie przewidują zmiany wynagrodzenia na podstawie ust. 11 niniejszego paragrafu w pierwszych 6 miesiącach wykonywania usługi. W kolejnych miesiącach wynagrodzenie będzie podlegało zmianie w wysokości wynikającej ze wskaźnika wzrostu GUS za poprzedni rok kalendarzowy z zastrzeżeniem ust. 15.
15. Maksymalna wartość zmiany wynagrodzenia, o której mowa w ust. 11-14 niniejszego paragrafu, wynosi łącznie 10% wartości wynagrodzenia brutto Wykonawcy, określonego w ust. 1 lit. f) Umowy.
16. Zmiana Umowy skutkuje zmianą wynagrodzenia jedynie w zakresie płatności realizowanych po dacie złożenia wniosku, pod warunkiem zawarcia aneksu do Umowy i zaakceptowaniu wniosków przez Zamawiającego.
17. Każda ze Strony jest uprawniona do wystąpienia z wnioskiem o zmianę wynagrodzenia. Postanowienia ust. 11-15 stosuje się odpowiednio do wniosku o zmniejszenie wynagrodzenia.
18. Wykonawca, którego wynagrodzenie zostało zmienione zgodnie z ust. 11-15 niniejszego paragrafu, zobowiązany jest do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom cen materiałów lub kosztów dotyczących zobowiązania podwykonawcy.

§ 7
Warunki gwarancji

1. Oprogramowanie PAM powinien być objęty 12 miesięczną gwarancją i wsparciem technicznym producenta oraz Wykonawcy.
2. Usługi w ramach gwarancji, w tym usuwanie Awarii, będą realizowane zgodnie z następującymi zasadami i terminami:
   a) czas reakcji – nie później niż w ciągu 1 godziny od momentu zgłoszenia wady oprogramowania PAM lub Awarii w sposób wskazany w § 4 ust. 3 Umowy do momentu potwierdzenia przyjęcia tego zgłoszenia, przesłanego na adres poczty elektronicznej Zamawiającego;

b) czas usunięcia wady Oprogramowania PAM lub Awarii – nie później niż w ciągu 24 godzin od momentu zgłoszenia wady Oprogramowania PAM lub Awarii w sposób wskazany w §4 ust. 3 Umowy do momentu potwierdzenia jej usunięcia przesłanego na adres poczty elektronicznej Zamawiającego. Jeśli po weryfikacji Zamawiający uzna, że dana wada Oprogramowania PAM lub Awaria nie została usunięta, to przysługuje mu prawo do zgłoszenia tego faktu w nowym zgłoszeniu wady Oprogramowania PAM lub Awarii, przy czym czas jej trwania liczy się jako kontynuacja pierwotnie zgłoszonej i nie usuniętej należycie wady lub Awarii;
c) w przypadku braku możliwości usunięcia wady lub Awarii w ciągu 24 godzin od momentu zgłoszenia, Zamawiający dopuszcza zastosowanie czasowego obejścia rozwiązania problemu w uzgodnieniu i za akceptacją Zamawiającego, jednak docelowe rozwiązanie problemu musi zostać dostarczone i zaimplementowane w czasie 30 dni liczonych od dnia następnego po dniu wdrożenia tymczasowego obejścia problemu.

3. Zakres usług wsparcia technicznego obejmuje:
   a) doradztwo i pomoc w zakresie obsługi Oprogramowania PAM;
   b) analizę i rozwiązywanie problemów związanych z Oprogramowania PAM oraz zaistniałych na styku pomiędzy Oprogramowaniem PAM i/lub Sprzętem Teleinformatycznym i innym oprogramowaniem użytkowanym przez Zamawiającego;
   c) zapewnienie dostępu (za pośrednictwem strony internetowej) i możliwości korzystania z aktualizacji, poprawek Oprogramowania PAM, nowych wersji oprogramowania, oraz dokumentacji administracyjnej i technicznej dotyczącej oprogramowania PAM;
   d) informowanie o znanych problemach z Oprogramowania PAM i sposobach ich rozwiązania drogą telefoniczną - lub poprzez pocztę elektroniczną.
4. W sytuacji, gdy pomoc Wykonawcy realizowana w ramach wsparcia technicznego, o którym mowa w ust. 2 i 3, okaże się niewystarczająca dla Zamawiającego, Wykonawca zobowiązuje do świadczenia na wniosek Zamawiającego usług wsparcia merytorycznego administratorów, o których mowa w § 2 ust. 1 pkt. 6), polegających na osobistym (bezpośrednim) wsparciu Zamawiającego w miejscu instalacji Oprogramowania PAM bądź w formie zdalnej przez wykwalifikowanych polskojęzycznych inżynierów w pełnym zakresie, w tym:
   a) usuwaniu Awarii na zasadach wskazanych Umowie.
   b) aktualizacji wersji wszystkich komponentów Oprogramowania PAM oraz przeprowadzania odpowiednich testów poprawnego funkcjonowania Oprogramowania PAM po ww. aktualizacjach;
   c) wdrażania nowych funkcjonalności Oprogramowania PAM, wynikających z ww. aktualizacji;
   d) pełnej instalacji i konfiguracji Oprogramowania PAM;
   e) oraz innych prac serwisowych dotyczących Oprogramowania PAM, na życzenie Zamawiającego.

§ 8
Kary umowne

1. Wykonawca zobowiązuje się do zapłaty Zamawiającemu następujących kar umownych w przypadku:
   1) niedotrzymania przez Wykonawcę terminu, o którym mowa w § 3 ust. 1 pkt. 1) Umowy – kwotę w wysokości 0,2 % wynagrodzenia, o którym mowa w § 6 ust. 1 Umowy za każdy rozpoczęty dzień zwłoki;
   2) niedotrzymania przez Wykonawcę terminu, o którym mowa w § 3 ust. 1 pkt. 2) Umowy – kwotę w wysokości 0,5 % wynagrodzenia, o którym mowa w § 6 ust. 1 Umowy za każdy rozpoczęty dzień zwłoki;

3) niedotrzymania przez Wykonawcę terminu, o którym mowa w § 3 ust. 1 pkt. 3) Umowy – kwotę w wysokości 0,2 % wynagrodzenia, o którym mowa w § 6 ust. 1 Umowy za każdy rozpoczęty dzień zwłoki;
4) niedotrzymania przez Wykonawcę terminu, o którym mowa w § 3 ust. 1 pkt. 4) Umowy – kwotę w wysokości 0,2 % wynagrodzenia, o którym mowa w § 6 ust. 1 Umowy za każdy rozpoczęty dzień zwłoki;
5) niedotrzymania przez Wykonawcę terminu, o którym mowa w § 3 ust. 2 Umowy – kwotę w wysokości 0,2 % wynagrodzenia, o którym mowa w § 6 ust. 1 Umowy za każdy rozpoczęty dzień zwłoki;
6) niedotrzymania przez Wykonawcę terminów, o którym mowa w § 7 ust. 2 Umowy – kwotę w wysokości 0,2 % wynagrodzenia, o którym mowa w § 6 ust. 1 Umowy za każdy rozpoczęty dzień zwłoki;
7) naruszenia postanowień § 11 Umowy – kwotę w wysokości 0,2% wynagrodzenia, o którym mowa w § 6 ust. 1 Umowy, za każde pojedyncze naruszenie;
8) naruszenia przez Wykonawcę wymogu zatrudnienia na podstawie umowy o pracę, o którym mowa w § 14 Umowy – kwotę w wysokości 1 000,00 zł za każde stwierdzone naruszenie.
9) odstąpienia od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy – kwotę w wysokości 20 % wynagrodzenia, o którym mowa w § 6 ust. 1 Umowy,

2. Sumaryczny limit kar umownych, jakie mogą być naliczone na podstawie Umowy, wynosi 100 % wynagrodzenia brutto, o którym mowa w § 6 ust. 1 Umowy.
3. W przypadku powstania szkody przenoszącej wysokość kar umownych określonych w Umowie, Zamawiający jest uprawniony do dochodzenia naprawienia szkody na zasadach ogólnych określonych w Kodeksie cywilnym.
4. W przypadku wystąpienia okoliczności uprawniających Zamawiającego do naliczenia Wykonawcy kary umownej, o której mowa w ust. 1 , Zamawiający naliczy karę umowną i wezwie Wykonawcę do jej zapłaty w terminie wskazanym w wezwaniu, nie krótszym niż 5 dni albo do przedstawienia w tym terminie wyjaśnień, oświadczeń lub dokumentów wskazujących na to, że do naruszenia doszło wskutek okoliczności, za które Wykonawca nie ponosi odpowiedzialności. W przypadku braku odpowiedzi Wykonawcy na wezwanie, o którym mowa w zdaniu poprzedzającym, Zamawiający uzna, że Wykonawca uznał zasadność i wysokość naliczonej mu kary umownej i uprawniony będzie do jej potrącenia z płatności faktury VAT wystawionej przez Wykonawcę, na co Wykonawca wyraża zgodę.

§ 9
Odstąpienia od Umowy

1. W przypadku niedotrzymania terminu, o którym mowa w § 3 Umowy, Zamawiający uprawniony jest do odstąpienia od Umowy, zgodnie z art. 492 k.c. i żądania kary umownej zgodnie z § 7 ust. 1 pkt 3 Umowy.
2. W przypadku częściowej realizacji Umowy Zamawiającemu przysługuje prawo odstąpienia od niezrealizowanej części Umowy. Wartość kary umownej należnej z tytułu odstąpienia od części Umowy zostanie obliczona na podstawie wartości wynagrodzenia należnego za niezrealizowaną część Przedmiotu Umowy.

§ 10
Dane adresowe

1. Wszelkie pisma i zawiadomienia związane z Umową będą przez Strony doręczane za pośrednictwem poczty elektronicznej na adresy przedstawicieli Stron, wskazanych w § 4 Umowy.
2. Pisma zmierzające do zmiany lub ustania łączącego Strony stosunku prawnego doręczane będą bezpośrednio do rąk drugiej Strony bądź wysyłane listem poleconym na następujące adresy:
   1) Zamawiający: Urząd Komunikacji Elektronicznej
      ul. Giełdowa 7/9, 01-211 Warszawa
   2) Wykonawca: …….
      …….
3. Strony zobowiązują się do wzajemnego informowania się o każdej zmianie danych wskazanych w ust. 2. W przypadku niezawiadomienia drugiej Strony o zmianie adresu, pismo przesłane na adres uprzednio wskazany, awizowane dwukrotnie, uznaje się za skutecznie doręczone.

§ 11
Poufność i ochrona danych

1. Wykonawca zobowiązuje się do:
   1) zachowania w tajemnicy wszelkich informacji uzyskanych w trakcie realizacji umowy niezależnie od formy przekazania tych informacji i ich źródła;
   2) wykorzystania informacji, o których mowa w pkt 1, jedynie w celach określonych w umowie;
   3) podejmowania wszelkich niezbędnych działań zapewniających, że żadna z osób uzyskujących informacje, o których mowa w pkt 1, nie ujawni tych informacji ani ich źródła zarówno w całości jak i w części osobom trzecim bez uzyskania uprzedniego pisemnego upoważnienia Zamawiającego;
   4) ujawniania informacji jedynie tym pracownikom Wykonawcy, którym ujawnienie takie będzie uzasadnione i tylko w zakresie, w jakim odbiorca informacji musi mieć do nich dostęp w związku z realizacją zadań służbowych związanych ze współpracą Stron;
   5) zapewnienia, aby pracownicy Wykonawcy, którym ujawniono informacje uzyskane w trakcie realizacji umowy, zachowali w tajemnicy te informacje, również po zakończeniu realizacji umowy, między innymi poprzez poinformowanie ich o prawnych konsekwencjach naruszenia poufności danych oraz odebranie od tych pracowników oświadczeń wraz z zobowiązaniem się do zachowania w tajemnicy tych danych.
2. Strony ustalają, że postanowienia ust. 1 nie mają zastosowania:
   1) do informacji ogólnie dostępnych oraz informacji, które stały się ogólnie dostępne nie za sprawą którejkolwiek ze Stron umowy;
   2) w przypadku, gdy odbiorcą informacji jest organ uprawniony do ich uzyskania zgodnie z przepisami powszechnie obowiązującego prawa;
   3) w przypadku informacji, które udostępnia się na mocy przepisów powszechnie obowiązującego prawa, w tym ustawy o dostępie do informacji publicznej.
3. Obowiązek zachowania tajemnicy będzie obowiązywał przez czas obowiązywania umowy, a po jej rozwiązaniu przez okres 2 lat z możliwością zastrzeżenia przez Zamawiającego przedłużenia okresu obowiązku zachowania tajemnicy w sytuacji, gdyby określone informacje nie straciły waloru tajemnicy prawnie chronionej.
4. Wykonawca zobowiązuje się w toku realizacji umowy przestrzegać obowiązujących u Zamawiającego zasad bezpieczeństwa i ochrony informacji.

5. Wykonawca jest zobowiązany do ustalenia z Zamawiającym sposobu przekazywania korespondencji zawierającej informacje mogące mieć wpływ na bezpieczeństwo informacji u Zamawiającego.
6. W razie wątpliwości, czy określona informacja stanowi tajemnicę Wykonawca zobowiązany jest zwrócić się w formie pisemnej do Zamawiającego o wyjaśnienie takiej wątpliwości.
7. Każda ze Stron zobowiązuje się do przestrzegania przepisów o ochronie danych osobowych, w szczególności przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1, z późn. zm.) – dalej „RODO".
8. Strony oświadczają, że dane kontaktowe reprezentantów Stron udostępniane wzajemnie w § 4 ust. 1 i 2 umowy lub udostępnione drugiej Stronie w jakikolwiek sposób w okresie obowiązywania umowy, przekazywane są w celu zapewnienia prawidłowej realizacji umowy. Udostępniane dane kontaktowe obejmują: imię i nazwisko, służbowy adres e-mail i służbowy numer telefonu. Każda ze Stron będzie administratorem danych kontaktowych, które zostały jej udostępnione w ramach umowy.
9. Wykonawca zobowiązuje się do przekazania w imieniu Zamawiającego wszystkim osobom, których dane osobowe udostępnił, informacji, o których mowa w art. 14 ust. 1 i 2 RODO, zgodnie z wzorem zamieszczonym w załączniku nr 3 do umowy (Klauzula informacyjna Zamawiającego dla osób reprezentujących Wykonawcę oraz wykonujących umowę ze strony Wykonawcy).

§ 12

Prawa autorskie

1. W ramach wynagrodzenia, o którym mowa w § 6 ust. 1, Wykonawca z dniem podpisania bez zastrzeżeń przez obie Strony Protokołu Odbioru Końcowego przenosi na Zamawiającego autorskie prawa majątkowe do wszelkiej Dokumentacji, powstałej w związku z realizacją przedmiotu Umowy, w zakresie wskazanym w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2021 r. poz. 1062 ze zm.), bez żadnych ograniczeń czasowych i terytorialnych, obejmujących w szczególności:
   1) w zakresie utrwalania i zwielokrotniania utworu - wytwarzanie określoną techniką egzemplarzy utworu, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
   2) w zakresie obrotu oryginałem albo egzemplarzami, na których utwór utrwalono - wprowadzanie do obrotu, użyczenie, dzierżawa lub najem oryginału albo egzemplarzy;
   3) w zakresie rozpowszechniania utworu w sposób inny niż określony w pkt 2 - publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym;
   4) odtwarzanie, przekazywanie, przechowywanie, wyświetlanie, wprowadzanie do pamięci komputera wraz z prawem do dokonywania modyfikacji;
   5) tłumaczenie, przystosowanie, zmiany układu lub jakiekolwiek inne zmiany.
2. Łącznie z przeniesieniem autorskich praw majątkowych, na Zamawiającego przechodzi wyłączne prawo do wykonywania i prawo zezwalania na wykonywanie autorskich praw

zależnych, w ramach których w szczególności Wykonawca wyraża zgodę na dokonywanie wszelkich przeróbek, zmian i aktualizacji utworu i wszelkich jego części objętych Umową w zakresie, w jakim Zamawiający uzna za celowe. Wykonawca nie ponosi odpowiedzialności za tak zmienione utwory, ani nie może być wskazywany jako ich autor.

3. Z chwilą przeniesienia majątkowych praw autorskich i praw zależnych do Dokumentacji, o której mowa w ust. 1, Wykonawca – w ramach wynagrodzenia, o którym mowa w § 6 ust. 1 Umowy - przenosi na Zamawiającego własność nośnika, na którym została ona utrwalona (zapisana) w chwili jej wydania, w przypadku gdy wydanie następuje w formie fizycznej, a nie poprzez jej udostępnienie w systemie informatycznym (w tym umożliwienie jej pobrania).
4. Wykonawca gwarantuje Zamawiającemu, że realizacja przedmiotu Umowy nie spowoduje naruszenia praw autorskich osób trzecich, znaków handlowych i towarowych, patentów, rozwiązań konstrukcyjnych i innych praw chronionych, w zakresie określonym Umową.
5. Wykonawca przejmuje na siebie wszelką odpowiedzialność za roszczenia osób trzecich w związku z realizacją Umowy, dotyczącą w szczególności naruszenia czyichkolwiek praw autorskich, znaków handlowych i towarowych, patentów, rozwiązań konstrukcyjnych oraz innych praw chronionych wyjątkiem roszczeń wynikających z wykorzystania dokumentów przekazanych przez Zamawiającego.
6. Wykonawca jako autor zobowiązuje się do niewykonywania nadzoru autorskiego nad stworzonymi w ramach Umowy utworami, lub jego częściami i wyraża nieodwołalną zgodę na swobodne rozporządzanie nimi przez Zamawiającego, a także na dokonywanie przez Zamawiającego wszelkich przeróbek, zmian i aktualizacji utworu i wszelkich jego części objętych Umową w zakresie, w jakim Zamawiający uzna za celowe z tym zastrzeżeniem, że w takim przypadku usunięcie lub pozostawienie nazwy Wykonawcy w zmienionym utworze będzie każdorazowo z nim uzgodnione i ma on prawo do żądania jej usunięcia lub pozostawienia, nie ograniczając jednocześnie praw autorskich osób, które dokonały zmian.
7. Wykonawca nie będzie ponosił odpowiedzialności za wyniki korzystania z utworów ze zmianami dokonanymi bez jego udziału.

§ 13

Zmiany umowy

1. Działając na podstawie art. 455 ust. 1 ustawy PZP Zamawiający przewiduje możliwość zmiany postanowień Umowy w następujących przypadkach:
   1) niezbędna jest zmiana terminu realizacji Umowy w przypadku zaistnienia okoliczności lub zdarzeń uniemożliwiających realizację Umowy w wyznaczonym terminie, o ile ich powstanie nie jest lub nie było w jakikolwiek sposób zależne od Wykonawcy. Zmianie może ulec termin realizacji Umowy o okres trwania zdarzenia lub okoliczności, o których mowa powyżej, a które uniemożliwiają realizację przedmiotu Umowy zgodnie z jej treścią i w sposób należyty;
   2) w przypadku zaistnienia innych okoliczności, bez względu na ich charakter, w tym leżących po stronie Zamawiającego, skutkujących niemożliwością wykonania lub należytego wykonania przedmiotu Umowy zgodnie z jej postanowieniami, o ile ich pojawienie się nie jest lub nie było w jakikolwiek sposób zależne od Wykonawcy, w tym o charakterze prawnym, organizacyjnym, ekonomicznym, administracyjnym lub technicznym, możliwa jest uzasadniona tymi okolicznościami zmiana:

a) sposobu wykonania Umowy, w tym zmiana zakresu lub wyłączenia części przedmiotu Umowy;
b) wynagrodzenia Wykonawcy przy czym wynagrodzenie może zostać zwiększone maksymalnie o 10% w stosunku do pierwotnie określonego Umową oraz zgodnie ze stawkami przyjętymi w ofercie Wykonawcy;
c) zmiana terminu realizacji przedmiotu Umowy odpowiednio do okresu trwania przeszkody, która uniemożliwia realizację przedmiotu Umowy, zgodnie z jej treścią i w sposób należyty;
3) zmiany wysokości wynagrodzenia w przypadkach określonych w § 6 ust. 11-18 Umowy;
4) zmiany wysokości wynagrodzenia w przypadkach określonych w ust. 2.

2. Zamawiający przewiduje dokonanie zmiany wysokości wynagrodzenia należnego Wykonawcy za realizację Umowy, każdorazowo w przypadku wystąpienia jednej z następujących okoliczności:
   1) zmiany stawki podatku od towarów i usług oraz podatku akcyzowego;
   2) zmiany wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. minimalnym wynagrodzeniu za pracę (Dz. U. z 2020 r. poz. 2207);
   3) zmiany zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne;
   4) zmiany zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (Dz. U. z 2020 r. poz. 1342 ze zm.);

- na zasadach i w sposób określony w ust. 3 – 13 jeżeli zmiany te będą miały wpływ na koszty wykonania Umowy przez Wykonawcę, o wartość wzrostu tych kosztów.

3. Zmiana wysokości wynagrodzenia w przypadku, o którym mowa w ust. 2 pkt 1) będzie dotyczyć wyłącznie części przedmiotu Umowy wykonanej w terminie przewidzianym Umową, po dniu wejścia w życie przepisów zmieniających stawkę podatku od towarów i usług lub podatku akcyzowego oraz wyłącznie do części przedmiotu Umowy, do której zastosowanie znajdzie zmiana stawki podatku od towarów i usług lub podatku akcyzowego.
4. W przypadku zmiany, o której mowa w ust. 2 pkt 1) wartość wynagrodzenia netto nie zmieni się, a wartość wynagrodzenia brutto zostanie wyliczona na podstawie nowych przepisów.
5. Zmiana wysokości wynagrodzenia w przypadku zaistnienia przesłanki, o której mowa w ust. 2 pkt 2), 3) lub 4) będzie obejmować wyłącznie część wynagrodzenia należnego Wykonawcy, w odniesieniu do której nastąpiła zmiana wysokości kosztów wykonania Umowy przez Wykonawcę w związku z wejściem w życie przepisów odpowiednio zmieniających wysokość minimalnego wynagrodzenia za pracę lub wysokość minimalnej stawki godzinowej, lub dokonujących zmian w zakresie zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub w zakresie wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne lub zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych.
6. W przypadku, o którym mowa w ust. 2 pkt 2), wynagrodzenie Wykonawcy ulegnie zmianie o kwotę odpowiadającą wzrostowi kosztu Wykonawcy w związku ze zwiększeniem wysokości wynagrodzeń lub wysokości minimalnej stawki godzinowej pracowników i osób

realizujących przedmiot Umowy, do wysokości aktualnie obowiązującego minimalnego wynagrodzenia za pracę lub minimalnej stawki godzinowej, z uwzględnieniem wszystkich obciążeń publicznoprawnych od kwoty wzrostu minimalnego wynagrodzenia lub minimalnej stawki godzinowej. Kwota odpowiadająca wzrostowi kosztu Wykonawcy będzie odnosić się wyłącznie do części wynagrodzenia pracowników i osób, o których mowa powyżej, realizujących przedmiot Umowy, odpowiadającej zakresowi, w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu Umowy wraz z pisemnym zestawieniem (zarówno przed jak i po zmianie) pracowników wykonujących przedmiot umowy z określeniem zakresu (części etatu).

7. W przypadku, o którym mowa w ust. 2 pkt 3) i 4), wynagrodzenie Wykonawcy ulegnie zmianie o kwotę odpowiadającą zmianie kosztu Wykonawcy ponoszonego w związku z wypłatą wynagrodzenia zaangażowanym przez Wykonawcę osobom realizującym przedmiot Umowy. Kwota odpowiadająca zmianie kosztu Wykonawcy będzie odnosić się wyłącznie do części wynagrodzenia osób, o których mowa powyżej, odpowiadającej zakresowi, w jakim wykonują one prace bezpośrednio związane z realizacją przedmiotu Umowy wraz z pisemnym zestawieniem (zarówno przed jak i po zmianie) z kwotami składek uiszczanych do zakładu Ubezpieczeń Społecznych/Kasy Rolniczego Ubezpieczenia Społecznego.
8. W celu zawarcia aneksu, o którym mowa w ust. 2, każda ze Stron, w terminie od dnia opublikowania przepisów dokonujących tych zmian, do 30 dnia od dnia ich wejścia w życie, może wystąpić do drugiej Strony z wnioskiem o dokonanie zmiany wysokości wynagrodzenia należnego Wykonawcy, wraz z uzasadnieniem zawierającym w szczególności szczegółowe wyliczenie całkowitej kwoty, o jaką wynagrodzenie Wykonawcy powinno ulec zmianie, oraz wskazaniem daty, od której nastąpiła bądź nastąpi zmiana wysokości kosztów wykonania umowy uzasadniająca zmianę wysokości wynagrodzenia należnego Wykonawcy.
9. W przypadku zmian, o których mowa w ust. 2 pkt 2) lub 3) lub 4), jeżeli z wnioskiem występuje Wykonawca, jest on zobowiązany dołączyć do wniosku dokumenty, z których będzie wynikać, w jakim zakresie zmiany te mają wpływ na koszty wykonania przedmiotu Umowy, w szczególności:
    1) pisemne zestawienie wynagrodzeń (zarówno przed jak i po zmianie obowiązujących przepisów) Pracowników świadczących Usługi, wraz z określeniem zakresu (części etatu), w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu Umowy oraz części wynagrodzenia odpowiadającej temu zakresowi - w przypadku zmiany, o której mowa w ust. 2 pkt 2), lub
    2) pisemne zestawienie wynagrodzeń (zarówno przed jak i po zmianie obowiązujących przepisów) pracowników świadczących usługi, wraz z kwotami składek uiszczanych do Zakładu Ubezpieczeń Społecznych/ Kasy Rolniczego Ubezpieczenia Społecznego w części finansowanej przez Wykonawcę, z określeniem zakresu (części etatu), w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu Umowy oraz części wynagrodzenia odpowiadającej temu zakresowi - w przypadku zmiany, o której mowa w ust. 2 pkt 3), lub
    3) pisemne zestawienie wynagrodzeń (zarówno przed jak i po zmianie obowiązujących przepisów) pracowników świadczących usługi, wraz z kwotami wpłat do pracowniczych planów kapitałowych dokonywanych przez Wykonawcę, z określeniem zakresu (części etatu), w jakim wykonują oni prace bezpośrednio

związane z realizacją przedmiotu Umowy oraz części wynagrodzenia odpowiadającej temu zakresowi - w przypadku zmiany, o której mowa w ust. 2 pkt 4).

10. W terminie 10 dni roboczych od dnia przekazania wniosku, o którym mowa w ust. 8, Strona, która otrzymała wniosek, przekaże drugiej Stronie informację o zakresie, w jakim zatwierdza wniosek oraz wskaże kwotę, o którą wynagrodzenie należne Wykonawcy powinno ulec zmianie, albo informację o niezatwierdzeniu wniosku wraz z uzasadnieniem.
11. W razie niezatwierdzenia wniosku lub częściowego zatwierdzenia wniosku, Strona może wniosek ponowić.
12. Każda ze zmian, o których mowa w niniejszym paragrafie, może skutkować obniżeniem wysokości wynagrodzenia Wykonawcy.
13. Zawarcie aneksu nastąpi nie później niż w terminie 10 dni roboczych od dnia zatwierdzenia wniosku o dokonanie zmiany wysokości wynagrodzenia należnego Wykonawcy. Aneks będzie obowiązywał od dnia jego zawarcia ze skutkiem od dnia wejścia w życie zmian przepisów będących podstawą do zmiany wysokości wynagrodzenia albo od dnia zawnioskowanego przez Stronę, jeżeli będzie to termin późniejszy.

§ 14

Zatrudnienie o pracę

1. Zamawiający wymaga zatrudnienia na podstawie umowy o pracę, w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. - Kodeks Pracy (Dz.U. z 2022 r. poz. 1510.), przez Wykonawcę co najmniej jednej osoby pełniącej funkcję Koordynatora odpowiedzialnego za prawidłową realizację zamówienia.

   Do zadań osoby pełniącej funkcję Koordynatora należało będzie w szczególności udzielanie natychmiastowej pomocy, jeśli pojawią się wątpliwości lub trudności przy realizacji zamówienia. Koordynator będzie udzielał Zamawiającemu wszelkich informacji związanych z organizacją wykonywanych usług w każdej sytuacji, gdy powstanie potrzeba przekazania uwag, wyjaśnienia wątpliwości, czy powzięcia przez Zamawiającego informacji o niezgodnych z warunkami umowy działaniach Wykonawcy. Koordynator dostępny będzie pod telefonem komórkowym i adresem e-mail. Koordynator na bieżąco będzie monitorował realizację obsługi zgłoszeń przekazanych przez osoby uprawnione oraz będzie kontrolował prawidłowość realizacji zamówienia przez Wykonawcę.
2. Wymóg zatrudnienia na podstawie umowy o pracę zostanie uznany za spełniony w przypadku osobistego wykonywania czynności wskazanych w § 13 ust. 1 Umowy przez osoby prowadzące indywidualną działalność gospodarczą
3. W trakcie realizacji Przedmiotu umowy Zamawiający uprawniony jest do wykonywania czynności kontrolnych wobec Wykonawcy odnośnie do spełniania przez Wykonawcę wymogu zatrudnienia na podstawie umowy o pracę osoby wskazanej w § 4 ust. 2 Umowy. Zamawiający uprawniony jest w szczególności do:
   a. żądania oświadczeń i dokumentów w zakresie potwierdzenia spełniania ww. wymogów i dokonywania ich oceny;
   b. żądania wyjaśnień w przypadku wątpliwości w zakresie potwierdzenia spełniania ww. wymogów.
4. Każdorazowo na żądanie Zamawiającego, w terminie wskazanym przez Zamawiającego, nie krótszym niż 2 dni robocze, Wykonawca zobowiązuje się przedłożyć dowód zatrudnienia w postaci oświadczenia o zatrudnieniu pracownika lub pracowników pełniących nadzór nad prawidłową realizacją umowy/zamówienia z powołaniem czasokresu zatrudnienia i jego wymiaru, a także

poświadczonych za zgodność z oryginałem przez Wykonawcę i zanonimizowanych kopii umów o pracę, zgodnie z powszechnie obowiązującymi przepisami o ochronie danych osobowych, zawartych przez Wykonawcę z ww. osobą lub osobami.

5. Nieprzedłożenie przez Wykonawcę w wyznaczonym przez Zamawiającego terminie dokumentów, o których mowa w niniejszym paragrafie, będzie traktowane jako niewypełnienie obowiązku zatrudnienia na podstawie umowy o pracę.
6. W przypadku uzasadnionych wątpliwości co do przestrzegania prawa pracy przez Wykonawcę Zamawiający może zwrócić się o przeprowadzenie kontroli przez Państwową Inspekcję Pracy.

§ 15

Postanowienia końcowe

1. Umowa zostaje zawarta z dniem jej podpisania przez obie Strony.
2. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron. / Umowę zawarto w formie elektronicznej i podpisano kwalifikowanym podpisem elektronicznym.
3. Wszelkie zmiany w treści Umowy wymagają zawarcia aneksu pod rygorem nieważności oraz mogą być dokonywane w zakresie i formie zgodnej z obowiązującymi przepisami.
4. Wykonawca nie może powierzyć wykonania Umowy osobie trzeciej, ani przenieść na nią swoich wierzytelności wynikających z Umowy, bez zgody Zamawiającego wyrażonej na piśmie.
5. Wszelkie spory czy roszczenia między Stronami wynikające z Umowy, powinny być rozwiązywane bez zbędnej zwłoki – drogą negocjacji między Stronami.
6. W przypadku niepowodzenia tych negocjacji, zaistniałe spory będzie rozstrzygał sąd właściwy miejscowo dla siedziby Zamawiającego.
7. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2022 r. poz. 1360).

ZAMAWIAJĄCY: **WYKONAWCA:**

7. Opis funkcjonalny Privileged Access Management (PAM):

Zarządzanie kontami i dostępami uprzywilejowanymi

1.54 Musi posiadać funkcje zarządzania (automatycznej zmiany haseł, definiowania polityki dostępu) kontami uprzywilejowanymi w:

j) Systemach operacyjnych: Windows, Unix, Linux (Debian, Ubuntu, RedHat), pSeries (AIX),

k) Bazach danych: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, DB2, MariaBD, MongoDB, PostgreSQL,

l) Systemach zarządzania infrastrukturą, aplikacjach: DELL DRAC, IBM Tivoli, RSA authentication Manager, HP iLO, SAP Application Server, MDM,

m) Urządzeniach sieciowych oraz systemach bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint, Netscreen, F5, Infoblox NIOS, FireEye Malware Analysis, FortiGate, Palo Alto Networks,

n) Narzędziach CI/CD: Chef, Jenkins, Kubernetes, Docker,

o) Aplikacjach typu SaaS/ stronach web/ interfejach web, minimum takich jak: Amazon Web Services (klucze API oraz konta uprzywilejowane, konto root), Zarządzanie Microsoft Azure (klucze API oraz konta uprzywilejowane),

p) Modułach: Microsoft Services, Scheduled tasks, IIS application Pool, IIS Directory Security, w rejestrach, COM+ , zarządzanie kontami w domenie Microsoft,

q) Plikach konfiguracyjnych, tabelach baz danych,

r) Środowiskach wirtualizacyjnych VMWare ESX/ESXi.

1.55 Musi zapewniać wsparcie (ochronę kont) dla dowolnego urządzenia obsługującego ODBC w wersji 2.7 lub wyższej.

1.56 Musi zapewniać wsparcie (możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego) dla systemów spoza listy "out of box" z wykorzystaniem skryptów lub innych mechanizmów realizowanych i wspieranych przez producenta rozwiązania dostępnych nieodpłatnie na oficjalnej stronie producenta rozwiązania. Producent powinien udostępniać nie mniej niż 200 unikalnych integracji udostępnionych w ramach wspomnianego portalu.

1.57 W przypadku ochrony kont lokalnych administratorów na stacjach roboczych Windows oraz MAC OS proponowane Musi obsługiwać scenariusz potencjalnej niedostępności stacji w momencie wykonania polityki automatycznej zmiany hasła lokalnego administratora (realizowanej przez narzędzie ochrony kont). W przypadku systemów, które często znajdują się poza siecią lokalną Zamawiającego musi istnieć możliwość wykorzystania narzędzia / agenta instalowanego na stacji roboczej, który będzie integrował się z proponowanym rozwiązaniem (w ramach tej samej subskrypcji) w celu zmiany hasła na stacji roboczej (gdy stacja zostanie podłączona do sieci lokalnej) i poinformowania narzędzia ochrony kont o realizacji zadania.

1.58 Musi zapewniać wsparcie (możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego) dla systemów spoza listy "out of box" z wykorzystaniem skryptów lub innych mechanizmów realizowanych i wspieranych przez producenta rozwiązania w zakresie zmiany haseł poprzez: SSH / Telnet, API do zewnętrznych aplikacji, możliwość wykonywania zmian oraz weryfikacji spójności haseł poprzez symulację działań użytkownika w sesji aplikacji Web.

1.59 Musi zapewniać możliwość automatycznego wykrywania kont w nowych urządzeniach Windows, usługach systemu Windows, zaplanowanych zadaniach, kontach serwisowych IIS itp., automatycznego dodania powyższych do produktu oraz automatycznie wymusić odpowiednią politykę zarządzania kontami uprzywilejowanymi.

1.60 Musi posiadać możliwość ochrony (zarządzania) oraz dynamicznego generowania (w formie pseudolosowej) nowego klucza SSH zgodne z określonym szablonem.

1.61 Musi automatycznie porównywać hasło/klucz SSH przechowywane w systemie oraz hasło/klucz SSH przechowywane na systemie docelowym.

1.62 Musi automatycznie synchronizować hasło (oraz klucz SSH) przechowywane w systemie oraz hasło (oraz klucz SSH) przechowywane na systemie docelowym w przypadku wykrycia niezgodności.

1.63 Musi umożliwiać przechowywanie historii rotacji haseł (np. trzy ostatnie hasła dla danego systemu docelowego) oraz umożliwiać łatwy dostęp do tej historii (np. poprzez interfejs webowy).

1.64 Musi wspierać różne środowiska LDAP do uwierzytelniania użytkowników, nie mniej niż Sun One, MS Active-Directory, IBM Tivoli, Novel eDirectory, Oracle Internet Directory

1.65 Musi umożliwiać wykrywanie par kluczy SSH w danej infrastrukturze.

1.66 Musi umożliwiać zarządzanie i zapewniać bezpieczeństwo kluczy SSH używanych przez aplikacje w przypadku przechowywania kluczy w plikach konfiguracyjnych.

1.67 Producent musi udostępniać bezpłatnie dodatkową aplikację umożliwiającą automatyzację procesu tworzenia nowych skryptów do rotacji poświadczeń w systemach docelowych dostępnych z wykorzystaniem protokołu SSH. Aplikacja musi umożliwiać nagranie procesu ręcznego logowania użytkownika do systemu docelowego i rotacji poświadczeń, a następnie na podstawie nagrania musi automatycznie wygenerować skrypt / plugin który będzie wykorzystany przez silnik automatycznego zarządzania poświadczeniami konta.

Zarządzanie sesjami uprzywilejowanymi

1.68 Musi umożliwiać zestawienie połączenia oraz monitoring sesji do systemu docelowego bez konieczności uprzedniego przekazania na stację użytkownika hasła konta uprzywilejowanego (po uwierzytelnieniu użytkownika oraz wskazaniu konta uprzywilejowanego produkt musi wprowadzić do dowolnie wybranej aplikacji dane dostępowe, dzięki czemu nie muszą być one udostępniane stacji użytkownika). Rozwiązanie musi udostępniać narzędzia do obsługi aplikacji instalowanych na systemie operacyjnym modułu separacji oraz nagrywania sesji. Jako obsługa rozumiane jest uruchomienie aplikacji oraz wypełnienie pól danymi dostępowymi automatycznie pobranymi z zabezpieczonego,

centralnego repozytorium kont uprzywilejowanych. W przypadku zestawienia połączeń przez przeglądarkę internetową narzędzie musi posiadać moduł umożliwiający realizację procesu utwardzania przeglądarki internetowej przez którą realizowana jest sesja uprzywilejowana (np. wyłączanie paska adresu, menu, narzędzi, widok theater mode, blokowanie wpisywania znaków podczas wypełniania danych dostępowych etc.).

1.69 Musi umożliwiać zestawianie i zarządzanie sesjami uprzywilejowanymi do systemów chronionych (w sposób opisany w punkcie 1.15 niniejszego dokumentu, nie jest dopuszczalne zestawianie połączeń do poniższych systemów poprzez wykorzystanie dodatkowych modułów pośredniczących klasy jumphost / bastion host, do których użytkownik może się interaktywnie zalogować, wybrać aplikacje i ręcznie zestawić sesję do systemu chronionego):

h) Musi posiadać wsparcie (dla monitoringu i separacji sesji oraz realizacji funkcji Single Systemach operacyjnych: Windows, Unix, Linux (Debian, Ubuntu, RedHat), pSeries (AIX),
i) Baz danych : Microsoft SQL, Oracle, MySQL, SAP HANA, DB2, PostgreSQL,
j) Systemów zarządzania infrastrukturą, aplikacji: DELL DRAC, RSA authentication Manager, HP iLO, SAP GUI, BMC Remedy,
k) Urządzeń sieciowych oraz systemów bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint (SmartDashboard, https, ssh), F5 Networks, FortiGate, Palo Alto Networks,
l) Narzędzi CI/CD (https, ssh): Chef, Jenkins, Kubernetes, Docker, Jfrog, GitHub,
m) Aplikacji typu SaaS/ stron web/ interfejsów web, minimum takich jak: Amazon Web Services (konsola zarządzania, IAM, integracja z STS), Zarządzanie Microsoft Azure
n) Środowisk wirtualizacyjnych VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh).

1.70 Sign-On dla kont uprzywilejowanych dla innych aplikacji oraz systemów niż wskazane w punkcie 1.16 poprzez możliwość wykorzystania nie mniej niż: uruchomienia aplikacji ze wskazanym zbiorem parametrów, zastosowania opisowego języka skryptowego, wbudowanego komponentu pozwalającego na obsługę własnych aplikacji web.

1.71 Producent musi udostępniać bezpłatnie dodatkową aplikację umożliwiającą automatyzację procesu tworzenia komponentów połączeniowych dla nowych / nieznanych aplikacji Web poprzez nagranie ręcznego połączenia użytkownika do aplikacji, automatyczną identyfikację nazw formularzy wykorzystywanych do wpisania poświadczeń przez użytkownika a następnie na podstawie nagrania automatyczne wygenerowanie odpowiedniego skryptu umożliwiającego połączenie zgodnie z opisem zawartym w punkcie 1.15 niniejszego dokumentu.

1.72 Musi przechowywać nagrania sesji w zabezpieczonym kryptograficznie repozytorium uniemożliwiającym ich manipulację. Żaden z użytkowników włącznie z administratorem systemu nie może mieć wpływu na integralność składowanych nagrań (włącznie z brakiem możliwości ich usunięcia w zdefiniowanym okresie składowania danych).

1.73 Musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie list dopuszczalnych i niedopuszczalnych poleceń wykonywanych poprzez SSH.

1.74 Musi zapewniać rozliczalność w przypadku jednoczesnego wykorzystania konta współdzielonego przez więcej niż jednego użytkownika.

1.75 Musi wykorzystywać mechanizmy indeksowania nagrań umożliwiające szybkie przeszukiwanie nagranych i monitorowanych sesji pod kątem występowania wskazanych słów kluczowych (wymagane są nie mniej niż następujące mechanizmy indeksowania: keystrokes, odpowiedzi okien systemu operacyjnego, komendy SQL). Nie jest dopuszczalnym dokonywanie indeksacji nagrań z wykorzystaniem mechanizmu OCR.

1.76 Musi umożliwiać wykorzystanie przez moduł proxy opisany w punkcie 1.15 funkcjonalności Microsoft Remote App w celu publikowania aplikacji dostępowych. Skrypty utwardzające (and. Hardening) muszą być dostarczone przez Producenta rozwiązania oraz uruchomione podczas instalacji rozwiązania.

1.77 Musi umożliwiać dostęp użytkowników do zasobu docelowego zgodnie z wymaganiami opisanymi w punkcie 1.15 przy wykorzystaniu nie mniej niż następujących metod / narzędzi:

e) interfejs Web proponowanego rozwiązania,

f) wykorzystanie różnych klientów RDP używanych na stacji, z której realizowany jest dostęp uprzywilejowany poprzez nie mniej niż: zdefiniowanie parametrów połączenia w ramach pliku konfiguracyjnego klienta RDP oraz możliwość interaktywnego odpytania użytkownika o właściwości systemu chronionego (takie jak adres, aplikacja kliencka, nazwa konta uprzywilejowanego) do którego będzie zestawione połączenie, przy czym wspierana musi metoda uwierzytelnienia do systemu bazująca na certyfikatach PKI,

g) wykorzystanie przeglądarki internetowej obsługującej html5 w celu zapewnienia wsparcia dla użytkowników korzystających z innych systemów operacyjnych niż Windows (brak klienta RDP na stacji użytkownika). W ramach połączenia realizowanego za pomocą tej metody sesja uprzywilejowana (zestawiona w oparciu o dowolną aplikację skonfigurowaną w systemie proxy, zgodnie z wymaganiami opisanymi w punkcie 1.15) musi być tunelowana w html5 i widoczna dla użytkownika jako nowa zakładka w przeglądarce,

h) Wykorzystanie różnych klientów linii poleceń i protokołu SSH (np. putty), przy czym wspierana musi metoda uwierzytelnienia do systemu bazująca na kluczach SSH.

1.78 Dla połączeń uprzywilejowanych zestawianych z poziomu interfejsu graficznego system musi umożliwiać wybór czy sesją ma być zestawiona ze stacji użytkownika w oparciu o protokół RDP czy protokół HTTPS (sesja tunelowana w html5 - mechanizm zestawiania sesji opisany w punkcie 1.24 podpunkt c),

1.79 Musi wspierać tryb automatycznego, tymczasowego przypisywania konta użytkownika systemu Windows do grupy lokalnych administratorów po złożeniu stosownego wniosku (tzw. tryb dostępu Just-in-time / JIT). Nadane przez proponowany System uprawnienia JIT muszą być automatycznie odbierane po upływie czasu, na który został nadany dostęp.

1.80 Musi wspierać tryb automatycznego generowania krótkoterminowych certyfikatów SSH w chronionych systemach Linux/Unix dla administratorów po złożeniu stosownego wniosku. Wygenerowane krótkoterminowe certyfikaty muszą być podpisane przez uprzednio

utworzony klucz CA oraz zawierać klucz publiczny, informację o tożsamości wnioskującego administratora i opcjonalnie dodatkowe restrykcje przypisanego do wnioskującego.

1.81 Musi umożliwiać transmisję plików oraz wykorzystanie schowka dla sesji tunelowanych w html5 (mechanizm zestawiania sesji opisany w punkcie 1.24 podpunkt c).

Zarządzanie incydentami bezpieczeństwa

1.82 Musi posiadać funkcję kategoryzacji nagranych sesji użytkowników pod kątem ryzyka. Ryzyko opisane musi być poprzez konfigurację przez administratora systemu zbioru wykrywanych w trakcie trwania sesji funkcji / poleceń i przypisanej do nich wagi. Ryzyko musi być analizowane i przypisane zarówno dla zakończonych jak i aktywnych sesji. Informacje dotyczące poziomu ryzyka sesji muszą być widoczne zarówno w konsoli monitoringu sesji jak i w interfejsie obrazującym ryzyko / incydenty bezpieczeństwa (dashboard). Administrator musi posiadać możliwość określenia akcji wykonanych przez użytkownika dla których sesja powinna być automatycznie zakończona / wstrzymana.

1.83 Musi posiadać wbudowane narzędzia analityczne umożliwiające automatyczne, bezobsługowe (bez konieczności definiowania reguł polityki bezpieczeństwa) wykrywanie podejrzanej aktywności kont uprzywilejowanych na bazie nauczonych automatycznie wzorców działania poszczególnych użytkowników (podejrzany czas pracy, nowy adres IP, zbyt duża ilość odwołań do repozytorium kont o hasła).

1.84 Musi umożliwiać pobieranie danych o aktywnościach użytkowników z zewnętrznych systemów SIEM, wspierane muszą być nie mniej niż następujące rozwiązania: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee, FortiSIEM oraz zewnętrzne źródła informacji, minimum rsyslog (z systemów Unix/Linux), Windows Event Forwarder (z systemów Windows), AWS CloudTrail, Azure Function App.

1.85 Musi umożliwiać podjęcie aktywnej akcji (co najmniej wymuszenie zmiany hasła konta uprzywilejowanego) w przypadku wykrycia anomalii wykorzystania kont uprzywilejowanych (nie mniej niż kradzież hasła konta uprzywilejowanego; utworzenie nowego konta i próba zestawienia nim połączenia z serwerem).

1.86 Musi generować odpowiedni alarm w przypadku wykrycia nadmiernego wykorzystania kont uprzywilejowanych przez danego użytkownika oraz w przypadku wykorzystania konta uprzywilejowanego w niestandardowych godzinach (np. poza typowymi dla danego użytkownika godzinami pracy).

1.87 Musi umożliwiać wykrywanie incydentów polegających na bezpośrednim dostępie użytkownika do systemu docelowego (np. bez wcześniejszego wysłania wniosku do proponowanego rozwiązania o hasło systemu docelowego) oraz na utworzeniu w systemie docelowym niezarządzanego do tej pory konta uprzywilejowanego. Rozwiązanie musi posiadać funkcje reagowania na tego typu działania poprzez wyegzekwowanie zmiany hasła konta uprzywilejowanego przez proponowany system, dodanie konta nowo utworzonego do centralnego repozytorium oraz automatyczny reset poświadczeń.

1.88 Musi wykrywać i wysyłać powiadomienia (alarmy) o wykrytych podatności środowiska dotyczących kont uprzywilejowanych: nieszyfrowana komunikacja do systemu pozwalająca na przejęcie danych dostępowych kont uprzywilejowanych, użycie kont serwisowych w

wielu celach (jako konta serwisowe i jednocześnie interaktywne), konta z włączoną funkcją "Unconstrained Delegation" oraz konta usług podatne na ataki klasy Kerberoasting (ang. risky SPNs).

1.89 Musi umożliwiać wykrywanie nowych, niezarządzanych kont uprzywilejowanych oraz połączeń, które zostały nawiązane bez uprzedniego pobrania hasła z centralnego repozytorium, realizowanych w środowisku AWS i Azure.

1.90 Musi umożliwiać monitoring, ingerencję oraz zakończenie aktywnej sesji graficznej w czasie jej trwania, a także określenie zbioru poleceń i uruchomionych funkcji systemu operacyjnego które spowodują automatyczne zakończenie / wstrzymanie sesji użytkownika (dla subskrypcji użytkownika wewnętrznego).

Architektura

1.91 Całość rozwiązania dostarczona musi być przez tego samego producenta, poszczególne moduły funkcjonalne muszą integrować się ze sobą.

1.92 Musi umożliwiać zainstalowanie bazy danych z centralnym repozytorium poświadczeń na odseparowanym, utwardzonym systemie operacyjnym, który nie będzie współdzielony z pozostałymi modułami rozwiązania (jak proxy izolujące sesje, interfejs graficzny, moduł rotacji poświadczeń czy silnik analityczny).

1.93 Musi posiadać budowę modularną, tzn. możliwość rozbudowy funkcjonalnej o kolejne komponenty, dostępne w ramach oddzielnych licencji/subskrypcji, odpowiedzialne za nie mniej niż:

- wieloskładnikowe uwierzytelnienie użytkowników (w tym przy wykorzystaniu kluczy sprzętowych) oraz zabezpieczenie dostępu do kluczowych aplikacji Web (wewnętrznych oraz chmurowych) poprzez moduł Single Sign-On (wymagania opisane w punkcie 2),
- ochronę dostępu zdalnego dla pracowników i zewnętrznych dostawców, wymagania opisane w punkcie 3,
- agentowe ograniczanie uprawnień użytkowników na stacjach Windows / MAC oraz serwerach Windows poprzez usuwanie kont lokalnych administratorów i podnoszenie uprawnień w kontekście konkretnych obiektów (skryptów, aplikacji, instalacji, dll i innych) dla konkretnych użytkowników, kontrolę aplikacyjną oraz blokowanie wycieku poświadczeń (np. haseł) z repozytoriów systemu operacyjnego Windows oraz aplikacji (np. przeglądarek internetowych, pamięci LSASS, SAM i innych),
- ochronę kont uprzywilejowanych w środowiskach DevOps,
- ochronę kont uprzywilejowanych zaszytych w kodzie statycznych aplikacji i skryptów,
- automatyczną klasyfikację ryzyka związanego ze zbyt obszernymi uprawnieniami w środowiskach chmurowych,
- automatyczne wykrywanie oraz reagowanie na ataki dotyczące kontrolerów domeny i protokołu kerberos (Overpass-the-hash, golden ticket, PAC manipulation, DCSync),
- agentowe ograniczanie dostępu do zbioru poleceń w połączeniach terminalowych do serwerów Linux/Unix (definiowanie centralnej polityki białych/czarnych list

wykonywanych poleceń, podnoszenia uprawnień poprzez sudo, rozliczania użytkowników z wykonanych zadań).

1.94 Producent musi udostępniać procedury opisujące sposób utwardzania każdego z komponentów Systemu oraz dostarczone w paczkach instalacyjnych skrypty automatyzujące proces utwardzania dostosowane do każdego z modułów funkcyjnych. Utwardzanie każdego z komponentów musi być realizowane w oparciu o dobre praktyki producenta systemu operacyjnego oraz producenta rozwiązania PAM/PAS. Utwardzanie systemu operacyjnego modułu repozytorium poświadczeń musi być realizowane automatycznie przez instalator podczas procesu instalacji modułu.

1.95 Zaproponowane rozwiązanie musi uwzględniać nie mniej niż: jeden moduł składowania danych (poświadczeń, nagrań sesji etc), 5x moduł składowania danych na potrzeby Disaster Recovery/High Availability, 5x moduł do zmian i zarządzania kluczami oraz hasłami w systemach chronionych, 2 środowiska testowe pozwalające na odwzorowanie środowiska produkcyjnego.

1.96 Rozwiązanie nie może ograniczać liczby modułów odpowiedzialnych za izolację, monitoring oraz rejestrację sesji a także interfejsów Web, którymi użytkownik może podłączyć się do systemu ochrony kont uprzywilejowanych (dodanie kolejnych modułów nie może wymagać zakupu dodatkowych licencji/subskrypcji producenta systemu ochrony kont uprzywilejowanych).

1.97 Musi wspierać rozproszoną architekturę, w której poszczególne moduły funkcyjne (proxy pośredniczące, moduły rotujące poświadczenia, interfejsy graficzne) zainstalowane są w wielu lokalizacjach (odseparowanych geograficznie) oraz komunikują się z elementami centralnymi (repozytorium poświadczeń) z wykorzystaniem bezpiecznego protokołu komunikacji zapewniającego bezpieczeństwo danych podczas transmisji, pracującego na jednym porcie TCP (do zadeklarowania podczas instalacji systemu). W przypadku infrastruktury rozproszonej całość systemu musi być zarządzana z centralnego interfejsu graficznego.

1.98 Zapewnienie wysokiej dostępności modułu składowania kont uprzywilejowanych musi być zaimplementowane na warstwie proponowanego oprogramowania (aplikacji), nie systemu operacyjnego/bazy danych, na którym oprogramowanie jest zainstalowane.

1.99 Produkt musi zapewniać ochronę kryptograficzną kopii zapasowych generowanych z produktu.

1.100 Rozwiązanie musi posiadać funkcję implementacji modułów składowania kont uprzywilejowanych w formie rozproszonej, złożonej z aktywnego modułu, redundancji modułu aktywnego oraz zbioru aktywnych modułów rozproszonych geograficznie, świadczących (w trybie odczytu) część funkcji użytkownikom (np. mechanizmy wykonywania kopii zapasowych, udostępniania danych kont uprzywilejowanych aplikacjom, dostęp do interfejsu użytkownika, możliwość zestawiania sesji uprzywilejowanych w sposób opisany w punkcie 1.15). Proponowane rozwiązanie musi obsługiwać nie mniej niż 6 aktywnych repozytoriów poświadczeń. W przypadku

infrastruktury rozproszonej całość systemu musi być zarządzana z centralnego interfejsu graficznego.

1.101 Rozwiązanie, w którym składowane są chronione konta uprzywilejowane musi uwzględniać zapasowe komponenty typu Disaster Recovery w lokalizacjach odseparowanych geograficznie. Musi istnieć możliwość wykorzystania trybu wysokiej dostępności (ang high availability) pomiędzy dwoma systemami współdzielącymi przestrzeń dyskową z zaszyfrowaną bazą danych oraz modułów zapasowych (ang. Disaster Recovery) w innych lokalizacjach (musi istnieć możliwość wdrożenia do 4 modułów Disaster Recovery w ramach podstawowej subskrypcji przy wdrożonym HA w lokalizacji podstawowej).

Integracje

1.102 Musi umożliwiać integrację z systemami SIEM w celu wysyłania informacji o zarejestrowanych zdarzeniach w ramach monitorowanych sesji. Musi istnieć możliwość zdefiniowania typu zdarzeń, które powinny być wysłane do systemu SIEM.

1.103 Musi wspierać integrację z rozwiązaniami typu HSM obsługującymi standard PKCS11, wymagana jest integracja z systemami: Atos HSM Proteccio, Gemalto Luna/Safenet 1700 Hardware Security Module, Thales nShield Hardware Security Module, Utimaco CryptoServer, Crypto4A QxEDGE, Fortanix SDKMS, i4p Trident, Unbound Key Control, Utimaco CryptoServer, HSM SafeNet ProtectServer External 2.

1.104 Musi umożliwiać integrację z mechanizmami wykorzystywanymi do uwierzytelniania użytkowników, minimum hasła, LDAP, Windows NTLM, klucze SSH, Smart card, PKI, RADIUS, SAML, wieloskładnikowe uwierzytelnianie, RSA SecurID, Oracle SSO, Amazon Cognito Authentication, OpenID Connect (OIDC), klucze YubiKey 5.

Wymagania dodatkowe

1.105 Musi posiadać skorelowaną ze sobą oficjalną metodykę implementacji, udostępnianą przez producenta systemu na stronie internetowej producenta. Metodyka ta musi zawierać minimum opis kroków, które należy wykonać w celu należytego i kompleksowego zaimplementowania rozwiązania typu PAS, umożliwiającego minimum ochronę dostępów uprzywilejowanych, wdrożenie polityki minimalnych uprawnień na stacjach roboczych i serwerach oraz ochronę kont uprzywilejowanych i danych uwierzytelniających wykorzystywanych przez aplikacje na potrzeby dostępu do innych systemów docelowych (włącznie z ochroną aplikacji wdrożonych w oparciu o metodykę DevOps). Metodyka poprzez analizę ryzyka musi umożliwiać pomoc w klasyfikacji kluczowych typów kont uprzywilejowanych oraz przypisanie ich do kolejnych etapów planowanej implementacji rozwiązania PAS. Metodyka musi być dostępna na oficjalnej stronie producenta na dzień składania ofert, link do oficjalnej strony producenta zawierającej opis metodyki należy dołączyć do oferty.

1.106 Proponowane Musi znajdować się w kwadracie "Leaders" raportu Gartner Magic Quadrant for Privileged Access Management za rok 2018, 2020 oraz 2021

8. Wieloskładnikowe uwierzytelnienie oraz zabezpieczenie dostępu do kluczowych aplikacji poprzez portal Single Sign-On

2.8 Musi realizować funkcję:

d) wieloskładnikowego adaptacyjnego uwierzytelnienia,

e) zabezpieczenia dostępu zarówno do wewnętrznych jak i zewnętrznych (SaaS) aplikacji poprzez wykorzystanie zabezpieczonego portalu SSO,

f) zarządzania cyklem życia tożsamości (ang. lifecycle management, wymagający dodatkowej subskrypcji).

2.9 Wymagana jest możliwość obsługi minimum następujących składników uwierzytelniających MFA: hasło, sms, email, oauth, aplikacja mobilna, phone call, pytanie bezpieczeństwa, Qrcode generowany w ramach procesu uwierzytelnienia do interfejsu Systemu, umożliwiający uwierzytelnienie użytkownika przy użyciu aplikacji mobilnej uprzednio zarejestrowanej w systemie, klucze sprzętowe YubiKey 5.

2.10 Musi wspierać kontekstowe uwierzytelnianie bazujące na minimum następujących warunkach: adres IP, dzień tygodnia, data, zakres dat, zakres czasu, adaptacyjnie poprzez automatyczną analizę zachowań użytkowników (profilowanie urządzenia, adresu IP).

2.11 Moduł MFA poprzez protokół Radius musi umożliwiać integrację z popularnymi koncentratorami VPN jak minimum Cisco Systems, Palo Alto Networks, Pulse Secure, Fortinet.

2.12 Musi być dostarczony jako usługa zewnętrzna (SaaS) wraz z modułem umożliwiającym integrację ze środowiskiem usług katalogowych AD/LDAP oraz uruchomienie serwera Radius dla klientów sieciowych Zamawiającego.

2.13 Musi realizować usługę SSO dla aplikacji chmurowych oraz wewnętrznych, realizując w sposób scentralizowany bezpieczne uwierzytelnienie przy wykorzystaniu metod opisanych w punktach 2.02 oraz 2.03. Musi istnieć możliwość integracji z własnymi aplikacjami poprzez nie mniej niż następujące integracje:

- plugin do przeglądarki,
- NTLM,
- Basic auth,
- Klient Oauth2,
- Serwer Oauth2,
- OpenID Connect,
- Saml,
- WS-Fed,
- Użytkownik – hasło.

2.14 Musi posiadać gotowe integracje SSO z nie mniej niż następującymi aplikacjami: Adobe Sign, Amazon Web Services, Box, Dropbox, NetSuite, Office 365, Salesforce, ServiceNow, Slack, Webex, Zendesk.

9. Ochrona dostępu zdalnego

3.12 Rozwiązanie musi realizować funkcję bezpiecznego, uprzywilejowanego dostępu zdalnego dla pracowników firm zewnętrznych (zwanego dalej Dostępem Zewnętrznym), bez konieczności instalacji rozwiązań klasy VPN (site-2-site lub client-site) po stronie sieci lub stacji roboczej firmy zewnętrznej.

3.13 Rozwiązanie nie może wymagać instalowania dodatkowego oprogramowania po stronie stacji roboczej użytkownika zewnętrznego poza przeglądarką internetową (wsparcie dla nie mniej niż przeglądarki Chrome, Edge, Firefox).

3.14 Proponowane rozwiązanie musi posiadać architekturę pozwalającą na zestawienie połączenia szyfrowanego pomiędzy stacją roboczą zewnętrznego dostawcy a siecią Zamawiającego bez konieczności otwierania ruchu przychodzącego do sieci Zamawiającego. W celu realizacji niniejszego punktu Rozwiązanie musi posiadać w swojej architekturze aplikację klasy SaaS (wymagane jest oferowanie przez Dostawcę aplikacji SaaS w rejonie Unii Europejskiej), do której z jednej strony zestawiany będzie ruch firm zewnętrznych, z drugiej zestawiane będzie bezpieczne połączenie z sieci Zamawiającego. Oprócz zwiększenia poziomu bezpieczeństwa Dostępu Zewnętrznego aplikacja musi realizować funkcję nadawania dostępu dla firm zewnętrznych, dzięki czemu Zamawiający będzie w stanie w trybie natychmiastowym (ang. Just-in-Time Provisioning) generować, akceptować i automatycznie wysyłać na podany podczas rejestracji adres e-mail wiadomości z zaproszeniem do zestawienia Dostępu Zewnętrznego. Aplikacja powinna umożliwiać zarządzanie utworzonymi użytkownikami (tworzenie nowych zaproszeń, nadawanie uprawnień, wyłączanie kont). Dostęp do aplikacji musi być możliwy poprzez wykorzystanie uwierzytelnienia biometrycznego, bez konieczności podawania danych dostępowych użytkownika (jak jego nazwa czy hasło).

3.15 Rozwiązanie musi obsługiwać uniwersalne uwierzytelnienie biometryczne (bez konieczności wpisywania przed zestawieniem połączenia danych dostępowych, jak użytkownik - hasło) realizowane przy użyciu stosowanych powszechnie urządzeń klasy smartphone.

3.16 Rozwiązanie musi posiadać wsparcie dla następujących platform mobilnych: IOS od wersji 10, Android od wersji 6.0. Dane biometryczne wykorzystywane do uwierzytelnienia składowane muszą być wyłącznie w modułach Secure Enclave / Trusted Execution Environment.

3.17 Oprócz realizacji funkcji uwierzytelnienia biometrycznego aplikacja mobilna Rozwiązania musi posiadać funkcję potwierdzenia tożsamości dla kluczowych operacji realizowanych przez aplikację SaaS, np. nadawanie uprawnień administracyjnych innym użytkownikom.

3.18 W celu obsłużenia całości ruchu uprzywilejowanego do sieci Zamawiającego przez przeglądarkę internetową. Rozwiązanie musi posiadać wsparcie tunelowania sesji graficznych RDP przy użyciu HTML5 oraz protokołu SDP, zgodnie z wymaganiami punktu 1.24 podpunkt c niniejszego dokumentu.

3.19 Rozwiązanie musi wspierać transfer plików w trakcie trwania sesji graficznej

3.20 Rozwiązanie musi posiadać interfejs REST API do automatyzacji procesu zarządzania użytkownikami.

3.21 Rozwiązanie musi wspierać konfigurację dla wielu instytucji, zarówno od strony Zamawiającego jak i zewnętrznych dostawców (Zamawiający może zarządzać dostępami wielu dostawców, dostawca potrzebuje wyłącznie jednej aplikacji na urządzeniu mobilnym by dostawać się do wielu Klientów, jeśli korzystają z tego samego rozwiązania)

3.22 Aplikacja mobilna Rozwiązania musi posiadać funkcję zapraszania innych użytkowników. Proces ten musi umożliwiać automatyczne założenie tożsamości użytkownika zewnętrznego w systemie PAS.

4. **Wdrożenie**

4.1. PAM musi być uruchomiony w następującym zakresie:

1) PAM musi być zainstalowany w najnowszej wersji wraz z najnowszymi aktualizacjami.

2) Konfiguracja Oprogramowania PAM musi uwzględniać:

a) Utworzenie kont użytkowników i grup w PAM zgodnie z wymaganiami Zamawiającego;

b) Integrację uwierzytelniania i autoryzacji użytkowników PAM z usługą katalogową Active Directory wykorzystywaną przez Zamawiającego;

c) Utworzenie kont systemów docelowych w PAM zgodnie z wymaganiami Zamawiającego;

d) Utworzenie polityk związanych ze złożonością hasła zgodnie z wymaganiami Zamawiającego;

e) Utworzenie harmonogramów zmiany hasła zgodnie z wymaganiami Zamawiającego;

f) Utworzenie schematów wnioskowania o dostęp do hasła i/lub sesji zgodnie z wymaganiami Zamawiającego;

3) Dołączenie PAM do systemu monitoringu (Zabbix) Zamawiającego. Wykonawca określi kluczowe mierniki odnośnie wydajności i dostępności Oprogramowanie PAM oraz określi wartości progowe dla tych liczników, dzięki którym możliwe będzie proaktywne monitorowanie PAM. W szczególności określone zostaną przez Wykonawcę dopuszczalne wartości wskaźników wydajnościowych wszystkich składników systemu w warunkach normalnych oraz ich wartości progowe, których przekroczenie będzie uznawane za sytuację alarmową i sytuację krytyczną.

4) Wykonanie testów akceptacyjnych:

e) Uruchamianie i zatrzymywanie rozwiązania PAM;

f) Weryfikacja procesu zarzadzania hasłami na kontach systemów docelowych;

g) Weryfikacja procesu zarzadzania sesjami;

h) Weryfikacja poprawności działania procedur;

5. **Instruktaż**

5.1. Zamawiający wymaga od Wykonawcy przeprowadzenia instruktażu dla 5 administratorów oprogramowania PAM.

5.2. Instruktaż odbędzie się w siedzibie Zamawiającego w uzgodnionym na roboczo pomiędzy Wykonawcą a Zamawiającym terminie. W przypadku gdy nie będzie możliwości zorganizowania instruktażu w siedzibie Zamawiającego, dopuszcza się zorganizowanie instruktażu w formie zdalnej.

5.3. Zamawiający wymaga aby instruktaż składał się z części teoretycznej i warsztatowej i trwał minimum 16 godzin (min. 2 dni robocze).

5.4. Zapewnienie infrastruktury dla części warsztatowej leży po stronie Wykonawcy.

5.5. Zakres szkolenia:

1) Ogólna architektura Oprogramowania PAM;

2) Bezpieczeństwo Oprogramowania PAM;

3) Konfiguracja kont systemów docelowych w Oprogramowaniu PAM;

4) Zarządzanie użytkownikami w Oprogramowaniu PAM i integracja z innymi mechanizmami uwierzytelnienia i autoryzacji;

5) Polityki złożoności hasła, harmonogram zmian haseł, walidacja poprawności zmiany hasła;

6) Zarządzanie sesjami w Oprogramowaniu PAM;

7) Zarządzanie schematami wnioskowania i akceptacji dostępu hasła i/lub sesji w Systemie PAM;

8) Audyt i raportowanie w Oprogramowaniu PAM;

9) Procedura aktualizacji Oprogramowania PAM;

10) Rozwiązywanie problemów;

6. **Gwarancja i wsparcie techniczne**

6.1. Oprogramowanie PAM powinien być objęty 12 miesięczną gwarancja i wsparciem technicznym producenta oraz Wykonawcy.

6.2. Usługi w ramach gwarancji, w tym usuwanie Awarii, będą realizowane zgodnie z następującymi zasadami i terminami:

1) czas reakcji – nie później niż w ciągu 1 godziny od momentu zgłoszenia wady oprogramowania PAM lub Awarii w sposób wskazany w §4 ust.3 Umowy do momentu potwierdzenia przyjęcia tego zgłoszenia, przesłanego na adres poczty elektronicznej Zamawiającego;

2) czas usunięcia wady Oprogramowania PAM lub Awarii – nie później niż w ciągu 24 godzin od momentu zgłoszenia wady Oprogramowania PAM lub Awarii w sposób wskazany w §4 ust.3 Umowy do momentu potwierdzenia jej usunięcia przesłanego na adres poczty elektronicznej Zamawiającego. Jeśli po weryfikacji Zamawiający uzna, że dana wada Oprogramowania PAM lub Awaria nie została usunięta, to przysługuje mu prawo do zgłoszenia tego faktu w nowym zgłoszeniu wady Oprogramowania PAM lub Awarii, przy czym czas jej trwania liczy się jako kontynuacja pierwotnie zgłoszonej i nie usuniętej należycie wady lub Awarii;

3) w przypadku braku możliwości usunięcia wady lub Awarii w ciągu 24 godzin od momentu zgłoszenia, Zamawiający dopuszcza zastosowanie czasowego obejścia rozwiązania problemu w uzgodnieniu i za akceptacją Zamawiającego, jednak docelowe rozwiązanie problemu musi

zostać dostarczone i zaimplementowane w czasie 30 dni liczonych od dnia następnego po dniu wdrożenia tymczasowego obejścia problemu

6.3. Zakres usług wsparcia technicznego obejmuje:

1) doradztwo i pomoc w zakresie obsługi Oprogramowania PAM;

2) analizę i rozwiązywanie problemów związanych z Oprogramowania PAM oraz zaistniałych na styku pomiędzy Oprogramowaniem PAM i/lub Sprzętem Teleinformatycznym i innym oprogramowaniem użytkowanym przez Zamawiającego;

3) zapewnienie dostępu (za pośrednictwem strony internetowej) i możliwości korzystania z aktualizacji, poprawek Oprogramowania PAM, nowych wersji oprogramowania, oraz dokumentacji administracyjnej i technicznej dotyczącej oprogramowania PAM;

4) informowanie o znanych problemach z Oprogramowania PAM i sposobach ich rozwiązania drogą telefoniczną - lub poprzez pocztę elektroniczną.

6.4. W sytuacji, gdy pomoc Wykonawcy realizowana w ramach wsparcia technicznego, o którym mowa w ust. 6.2 i 6.3, okaże się niewystarczająca dla Zamawiającego, Wykonawca zobowiązuje do świadczenia na wniosek Zamawiającego dodatkowych usług wsparcia merytorycznego w wymiarze 160 godzin przez okres 12 miesięcy, polegających na osobistym (bezpośrednim) wsparciu Zamawiającego w miejscu instalacji Oprogramowania PAM bądź w formie zdalnej przez wykwalifikowanych polskojęzycznych inżynierów w pełnym zakresie, w tym:

1) usuwaniu Awarii na zasadach wskazanych OPZ oraz Umowie.

2) aktualizacji wersji wszystkich komponentów Oprogramowania PAM oraz przeprowadzania odpowiednich testów poprawnego funkcjonowania Oprogramowania PAM po ww. aktualizacjach;

3) wdrażania nowych funkcjonalności Oprogramowania PAM, wynikających z ww. aktualizacji;

4) pełnej instalacji i konfiguracji Oprogramowania PAM;

5) oraz innych prac serwisowych dotyczących Oprogramowania PAM, na życzenie Zamawiającego.

Załącznik nr 2 do Umowy

PROTOKÓŁ ODBIORU

z dnia ……2022 r.

Zamawiający:
Urząd Komunikacji Elektronicznej, ul. Giełdowa 7/9, 01-211 Warszawa
Wykonawca:
…….

Realizując postanowienia Umowy nr: …… z dnia ……..2022 r. Zamawiający przyjmuje do odbioru:

Lp.	Wyszczególnienie	Wartość brutto (zł)
1.	…….....	**……. zł**

1. Dokumenty przekazane przy odbiorze:
   -
2. Osoby uczestniczące w odbiorze:
   Przedstawiciele Zamawiającego:
   -
   Przedstawiciel Wykonawcy:
   -
3. Uwagi
   - ……
4. Protokół sporządzono w dwóch egzemplarzach, po jednym dla każdej ze Stron.
5. Na tym protokół zakończono i podpisano.

Zamawiający:	Wykonawca:
……	……
(podpis)	*(podpis)*
……	……
(data)	*(data)*

Załącznik nr 3 do Umowy

Klauzula informacyjna Zamawiającego dla osób reprezentujących Wykonawcę oraz wykonujących umowę ze strony Wykonawcy

Na podstawie art. 14 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) „RODO", informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest Prezes Urzędu Komunikacji Elektronicznej z siedzibą w Warszawie, ul. Giełdowa 7/9, 01-211 Warszawa.

   Dane kontaktowe: Urząd Komunikacji Elektronicznej (UKE), numer telefonu: +48 22 33 04 000, numer faksu: +48 22 53 49 162, formularz kontaktowy dostępny na stronie http://uke.gov.pl/kontakt/
2. Dane kontaktowe Inspektora Ochrony Danych: numer telefon: +48 22 53 49 241, e-mail: iod@uke.gov.pl.
3. Prezes UKE przetwarza Pani/Pana dane osobowe (dane kontaktowe obejmujące imię i nazwisko, adres e-mail, numer telefonu), które otrzymał od … …. … z siedzibą w … … … , w celu realizacji zawartej umowy na uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze UKE.
4. Pana/Pani dane osobowe będą przetwarzać upoważnieni pracownicy Administratora, którzy w ramach wykonania swoich obowiązków służbowych muszą posiadać do nich dostęp.
5. Dane osobowe przetwarzane przez Prezesa UKE mogą być udostępniane innym odbiorcom danych osobowych lub kategoriom odbiorców:
   a) podmiotom, które przetwarzają dane w imieniu Prezesa UKE na podstawie zawartej umowy powierzenia przetwarzania danych osobowych (np. podmioty obsługujące systemy teleinformatyczne UKE lub udostępniające UKE narzędzia teleinformatyczne, podmioty obsługujące i utrzymujące sieć telekomunikacyjną UKE, podmioty świadczące na rzecz UKE usługi doradcze, audytowe i pomoc prawną),
   b) innym administratorom przetwarzającym dane we własnym imieniu (np. podmioty prowadzące działalność pocztową lub kurierską).

   Dane osobowe przetwarzane przez Prezesa UKE mogą być również udostępniane podmiotom upoważnionym do odbioru danych na podstawie odpowiednich przepisów prawa (np. organy administracji, sądy, służby państwowe).
6. Dane osobowe są przetwarzane przez okres niezbędny do wykonania i rozliczenia umowy, a następnie do celów archiwalnych przez okres przewidziany w przepisach kancelaryjno-archiwalnych UKE, przyjętych zgodnie z ustawą o narodowym zasobie archiwalnym i archiwach.
7. W związku z przetwarzaniem przez Prezesa UKE danych osobowych przysługuje Pani/Panu:
   a) prawo do uzyskania potwierdzenia, czy Prezes UKE przetwarza Pani/Pana dane osobowe, a jeżeli ma to miejsce uzyskanie dostępu do treści tych danych oraz informacji dotyczących takiego przetwarzania,
   b) prawo do uzyskania kopii danych osobowych,
   c) prawo do sprostowania nieprawidłowych lub uzupełnienia niekompletnych danych, na podstawie i zasadach określonych w art. 16 RODO,
   d) prawo do ograniczenia przetwarzania danych, na podstawie i zasadach określonych w art. 18 RODO.

   Z tych praw może Pani/Pan skorzystać wysyłając e-maila na adres: iod@uke.gov.pl.

   Przepisy RODO określają zakres, w jakim można skorzystać z wyżej wymienionych praw. Prezes UKE jest uprawniony do weryfikacji tożsamości wnioskujących.

8. Przysługuje Pani/Panu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, na niezgodne z prawem przetwarzanie przez Prezesa UKE danych osobowych.
9. Prezes UKE nie dokonuje zautomatyzowanego podejmowania decyzji, w tym profilowania, w odniesieniu do Pani/Pana danych osobowych w ten sposób, że w wyniku takiego zautomatyzowanego przetwarzania mogłyby zapadać jakiekolwiek decyzje, miałyby być powodowane inne skutki prawne lub w inny sposób miałoby to istotnie wpływać na Pani/Pana sytuację.

Znak sprawy: BA.WZP.26.44.2022

Załącznik nr 7 do SWZ

Nazwa Wykonawcy: Kliknij tutaj, aby wprowadzić tekst.

Adres Wykonawcy: Kliknij tutaj, aby wprowadzić tekst.

O Ś W I A D C Z E N I E O B R A K U P O D S T A W W Y K L U C Z E N I A
na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. poz. 835).

Dotyczy postępowania o udzielenie zamówienia publicznego pn.
„Uruchomienie licencji rozwiązania Privilege Access Management (PAM) w infrastrukturze Zamawiającego"

Przystępując do prowadzonego postępowania o udzielenie ww. zamówienia publicznego oświadczam, że:

☐ **nie podlegam wykluczeniu z postępowania** na podstawie przesłanek wskazanych w przepisach art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).

☐ **zachodzą w stosunku do mnie podstawy wykluczenia z postępowania** na podstawie art. …….. (należy wpisać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835))*

** należy zaznaczyć odpowiednie pole wyboru*

Podpisy osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy

……

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym.

W przypadku składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenie składa każdy z tych Wykonawców (np. członek konsorcjum, wspólnik w spółce cywilnej).