Znak sprawy: BA.WZP.26.44.2022

Załącznik nr 6 do SWZ PO ZMIANIE

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:
   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.

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 **do 20.12.2022 r.** .
    2) uruchomienie i konfiguracja PAM w środowisku Zamawiającego w terminie **do 10.03.2023 r.**;
    3) przeprowadzenie instruktażu dla Zamawiającego z uruchomienia, konfiguracji i administracji PAM w terminie **do 31.03.2023 r.**;
    4) sporządzenie i dostarczenie Zamawiającemu Dokumentacji Powykonawczej w terminie **do 31.03.2023 r.**;
    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, licząc od dnia podpisania Końcowego Protokołu Odbioru.
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 nastąpi w dwóch transzach, tj.:
    a) pierwsza transza dotyczy płatności, o których mowa w ust. 1 lit. a), c) i f), co zostanie potwierdzone protokołem odbioru;
    b) druga transza dotyczy płatności, o których mowa w ust. 1 lit. b), d) i e), 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. 5, 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. 7 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.

5. W przypadku gdy usterka PIM/PAM wymaga opracowania przez producenta zmian w oprogramowaniu PIM/PAM (np. opracowanie zmian konfiguracyjnych pomiędzy komponentami oprogramowania PIM/PAM, wydania przez producenta tzw. patch'a lub fix'a do oprogramowania lub innych zmian wymagających ingerencji producenta w kod źródłowy lub inne komponenty oprogramowania PIM/PAM), zgłoszenie usterki procedowane jest zgodnie z warunkami i terminami świadczenia serwisu gwarancyjnego producenta PIM/PAM. Powyższe nie zdejmuje z Wykonawcy obowiązku dołożenia najwyższej staranności mającej na celu naprawę lub zastosowanie obejścia, w tym:
   i. zebranie i dostarczenie informacji działowi wsparcia producenta PIM/PAM;
   ii. monitorowania czasów odpowiedzi producenta PIM/PAM oraz eskalacji opóźnień;
   iii. instalacji w obecności personelu Zamawiającego na środowiskach testowych i produkcyjnych poprawek (patchy) dostarczonych przez producenta PIM/PAM (chyba że Zamawiający wskaże środowiska, na których instalacja będzie realizowana bezpośrednio przez Zamawiającego);
   iv. testowania poprawek dostarczonych przez producenta PIM/PAM.

§ 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 § 14 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:**

Załącznik nr 1 – Opis Przedmiotu Umowy.

1. Opis funkcjonalny Privileged Access Management (PAM):

Zarządzanie kontami i dostępami uprzywilejowanymi

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

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

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

1.9 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 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 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 Musi umożliwiać wykrywanie par kluczy SSH w danej infrastrukturze.

1.13 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 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 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):

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

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

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

1.39 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 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 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 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 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 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.

1.48 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 Rozwiązania 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 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 Rozwiązanie musi wspierać transfer plików w trakcie trwania sesji graficznej

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

3.10 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)

3.11 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:

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.

Załącznik nr 2

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

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.