UMOWA Nr .....

zawarta w dniu ..... w Warszawie pomiędzy:

Skarbem Państwa - Kasą Rolniczego Ubezpieczenia Społecznego, z siedzibą w Warszawie przy Al. Niepodległości 190, 00–608 Warszawa, NIP 526-00-13-054, REGON 012513262, reprezentowaną przez:

..... Biura Informatyki i Telekomunikacji na podstawie pełnomocnictwa Prezesa Kasy Rolniczego Ubezpieczenia Społecznego nr ..... z dnia .....
zwanym w treści Umowy „Zamawiającym",

a

.....z siedzibą:....., wpisaną do pod numerem KRS..... , NIP....., REGON..... ,
reprezentowaną przez:

.....
zwanym w treści Umowy „Wykonawcą",
Zamawiający i Wykonawca zwani łącznie w treści Umowy Stronami,

w wyniku przeprowadzenia uproszczonego postepowania do którego na podstawie art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2019 r. poz. 1843) nie stosuje się przepisów niniejszej ustawy, zawarto umowę następującej treści:

§ 1
PRZEDMIOT UMOWY

1. Wykonawca zobowiązuje się do dostarczenia licencji oprogramowania do zarządzania kontami uprzywilejowanymi (PAM) wraz z dożywotnią aktualizacją (dalej zwaną jako ATiK) na potrzeby realizacji zadań Biura Informatyki i Telekomunikacji w ilości 20 szt.
2. Szczegółowy opis przedmiotu zamówienia oprogramowania PAM, określony został w Załączniku nr 2 do niniejszej Umowy.
3. Wykonawca zobowiązuje się w ramach zamówienia do dostawy, instalacji oraz wdrożenia systemu PAM.
4. Wszystkie licencje udzielane na oprogramowania, o których mowa w ust. 1, są licencjami niewyłącznymi i bezterminowymi, udzielonymi/wystawionymi Zamawiającemu. W przypadku, gdy umowa licencyjna producenta oprogramowania dopuszcza możliwość wypowiedzenia licencji, Zamawiający dopuszcza wypowiedzenie licencji jedynie na warunkach wskazanych w tej umowie licencyjnej.

§ 2
ZASADY REALIZACJI

1. Wykonawca zobowiązuje się zrealizować całość przedmiotu Umowy w terminie do dnia 31.12.2019 r. oraz świadczyć wsparcie techniczne przez jeden rok od momentu wdrożenia, w języku polskim w trybie 8x5 z czasem reakcji na zgłoszenie: 1 godzina.
2. Prawidłowa realizacja dostawy licencji oraz wykonania usługi dostawy, instalacji oraz wdrożenia systemu PAM, będącej przedmiotem umowy potwierdzona zostanie Protokołem odbioru, którego wzór stanowi Załącznik nr 1 do niniejszej Umowy.
3. W ramach ATiK Zamawiający nabędzie uprawnienia zdefiniowane przez producenta oprogramowania w ramach ww. usługi, w szczególności prawa co najmniej do:
    a) pobierania od producenta w postaci elektronicznej nowych wersji posiadanego oprogramowania,
    b) pobierania od producenta poprawek i łatek do posiadanego oprogramowania bez dodatkowych opłat licencyjnych,
    c) zgłaszania problemów i uzyskiwania pomocy technicznej od producenta w zakresie problemów, wad i błędów wykrytych w oprogramowaniu bezpośrednio od producenta,
    d) dostępu do bazy wiedzy producenta w zakresie posiadanego oprogramowania.
4. Usługa ATiK świadczona będzie co najmniej za pomocą następujących kanałów:
    a) za pomocą dedykowanego do świadczenia pomocy technicznej systemu internetowego producenta: .....
    b) za pomocą poczty elektronicznej–adres: .....
5. Poziom świadczonej usługi ATiK dla całości wyszczególnionego oprogramowania określony jest na poziomie – Pro Support.
6. Wykonawca gwarantuje, że realizacja niniejszej umowy nie spowoduje naruszenia czyichkolwiek praw autorskich, znaków handlowych, towarowych, patentów, rozwiązań konstrukcyjnych oraz innych praw chronionych.
7. Wykonawca przyjmuje na siebie wszelką odpowiedzialność za naruszenie praw osób trzecich w związku z realizacją umowy, dotyczącą w szczególności naruszenia czyichkolwiek praw autorskich.
8. Na mocy niniejszej umowy Wykonawca udziela Zamawiającemu, na czas nieokreślony prawa do korzystania z oprogramowania określonego w § 1 na następujących polach eksploatacji:
    a) prawo do korzystania ze wszystkich funkcjonalności dostarczonego oprogramowania w dowolny sposób w liczbie kopii/ stanowisk/ serwerów/ użytkowników charakterystycznej dla dostarczonego oprogramowania zgodnie z opublikowanymi przez producenta warunkami licencyjnymi,
    b) prawo do instalowania dostarczonego oprogramowania w liczbie kopii/ stanowisk/ serwerów/użytkowników charakterystycznej dla odsprzedawanego oprogramowania zgodnie z opublikowanymi przez producenta warunkami licencyjnymi,
    c) prawo do instalowania wszelkich poprawek opublikowanych na stronach producenta oprogramowania oraz polach eksploatacji określonych w opublikowanych przez producenta warunkach licencyjnych.

§ 3
WYNAGRODZENIE I ZASADY PŁATNOŚCI

1. Wynagrodzenie całkowite Wykonawcy za realizację przedmiotu umowy nie przekroczy kwoty ..... zł netto (słownie: .....zł 00/100) plus podatek VAT w wysokości 23%, co stanowi kwotę ..... zł brutto (słownie: ..... zł 00/100).
2. Cena za jedną licencję oprogramowania wynosi ..... zł brutto (słownie: .....zł 00/100), w tym podatek VAT (23%).
3. Płatność wynagrodzenia nastąpi w formie przelewu bankowego na rachunek bankowy Wykonawcy, wskazany w fakturze VAT, w terminie 14 dni od daty dostarczenia do siedziby Zamawiającego poprawnie wystawionego oryginału faktury VAT wraz z oryginałem Protokołu odbioru podpisanym bez zastrzeżeń przez upoważnionych przedstawicieli Stron.
4. Podstawą do zapłaty faktury VAT będzie oryginał Protokołu odbioru podpisany bez zastrzeżeń, o którym mowa w § 2 ust. 2 niniejszej Umowy.
5. Za dzień płatności przyjmuje się dzień obciążenia rachunku bankowego Zamawiającego należną Wykonawcy kwotą.
6. Wraz z fakturą Wykonawca przedstawi Zamawiającemu w formie pisemnej, elektronicznej lub dokumentowej informację o liczbie godzin wykonywania niniejszej umowy, w przypadku, kiedy Wykonawca podlega przepisom ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U z 2018 r. poz. 2177).
7. Zamawiający nie wyraża zgody na cesję wierzytelności wynikających z Umowy.

§ 4
ODSTĄPIENIE I KARY UMOWNE

1. Oprócz przypadków przewidzianych w ustawie z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2019 r. poz. 1145), Zamawiającemu przysługuje prawo do odstąpienia od umowy w całości lub części:
   1) w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwa publicznemu - odstąpienie od umowy w tym wypadku może nastąpić w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach,
   2) w przypadku gdy Wykonawca nie zrealizuje przedmiotu umowy w terminie określonym w § 2 ust. 1 – odstąpienie od umowy w tym wypadku może nastąpić w okresie 30 dni po przekroczeniu powyższego terminu.
2. W przypadku odstąpienia od Umowy przez Wykonawcę lub Zamawiającego z powodu okoliczności zależnych od Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 5% wynagrodzenia brutto wymienionego w § 3 ust. 1 umowy.
3. Zamawiający może dochodzić odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych.
4. Wykonawca wyraża zgodę na potrącanie kar umownych z przysługującego mu wynagrodzenia.

§ 5
POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych w Umowie mają zastosowanie odpowiednie przepisy Kodeksu cywilnego oraz inne przepisy mające związek z realizacją Umowy.
2. Załączniki do niniejszej Umowy stanowią jej integralną część.
3. Wszelkie ewentualne spory mogące wynikać przy realizacji niniejszej umowy będą podlegały rozstrzygnięciu przez sąd właściwy miejscowo dla siedziby Zamawiającego.
4. Wszelkie zmiany i uzupełnienia Umowy wymagają formy pisemnej pod rygorem nieważności.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Wykaz załączników:
Załącznik nr 1 - Protokół odbioru prac.
Załącznik nr 2 – Opis przedmiotu zamówienia oprogramowania PAM.

Zamawiający: **Wykonawca:**

Elżbieta Artwich
RADCA PRAWNY
BŁ/S/127
20.11.2019

Załącznik nr 1
do umowy nr .....
z dnia .....

Warszawa, dnia .....

Protokół odbioru

W dniu .....w siedzibie ..... dokonano odbioru ..... w ramach umowy nr ..... z dnia .....

Niniejszy Protokół odbioru jest podstawą do zapłaty faktury za wykonaną dostawę.

Dostawa została przyjęta (nieprzyjęta)* ze względu na .....
.....
.....
.....

Wykonawca **Zamawiający**

....

*/ niepotrzebne skreślić

Załącznik nr 2
do umowy nr .....
z dnia .....

Opis przedmiotu zamówienia oprogramowania PAM

(Privileged Access Management)

1. **Skalowalność oprogramowania i wsparcie techniczne:**

1.1. Liczba krytycznych systemów docelowych objętych systemem PAM: 20 (dwadzieścia).
1.2. Systemy, które zostaną objęte systemem PAM: Windows Server, Linux.
1.3. Jeden rok, wsparcia świadczonego w języku polskim w trybie 8x5, dostęp do aktualizacji i poprawek producenta oferowanego systemu, czas reakcji na zgłoszenie: jedna godzina.

Wymagania techniczne dla systemu PAM:

1. Architektura:

Oferowany system musi być w postaci zamkniętej platformy wirtualnej, przygotowanej do implementacji w infrastrukturze. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizujące funkcjonalności systemu PAM. Zamawiający zapewni infrastrukturę wymaganą do instalacji maszyny wirtualnej.
Oferowany system musi zarządzać kontami na systemach docelowych w modelu bezagentowym.
Interfejs użytkownika oferowanego systemu PAM musi być dostępny przez przeglądarkę internetową HTTPS/TLS.
Hasła przechowywane w oferowanym systemie PAM muszą być szyfrowane (AES256) .
Oferowany system PAM musi zapewniać rozdzielenie obowiązków (Segregation of Duties), egzekwowane za pomocą kontroli dostępu opartej na rolach.

2. Uwierzytelnianie, autoryzacja i separacja uprawnień:

System musi umożliwiać integracje kont użytkowników systemu PAM z mechanizmami uwierzytelniania Active Directory wykorzystanie dwuskładnikowego uwierzytelniania (RADIUS) do portal PAM.
System musi umożliwiać rozdzielenie ról: wnioskujący (operator lub administrator danego systemu docelowego, wnioskujący o dostęp do sesji i haseł), administrator (zarządzający systemem PAM), audytor (uprawniony do monitoringu i przeglądania sesji i logów), zatwierdzający (zatwierdzający wnioski o dostęp do sesji i haseł).
System musi umożliwiać nadanie użytkownikowi kilku ról rozgraniczenie dostępu użytkowników (dla ról wnioskujący, audytor, zatwierdzający) wyłącznie do wskazanych kont systemów docelowych.

3. Konta systemów docelowych:

System musi posiadać wsparcie dla zarządzania kontami uprzywilejowanymi na docelowych systemach operacyjnych, takich jak: AIX, Unix, Linux, Mac OSX, Solaris, Windows, Oracle, MS-SQL, Cisco, Fortinet, Juniper, Palo Alto Networks, vSphere. System musi posiadać wsparcie dla

zarządzania kontami uprzywilejowanymi w bazach danych, takich jak: Oracle, MS SQL Server Server, MySQL, Sybase ASE, PostgreSQL, MongoDB.
System musi posiadać wsparcie dla zarządzania kontami uprzywilejowanymi w urządzeniach, takich jak: Cisco, Dell iDRAC, BIG-IP, HP iLo, HP Comware, Juniper, Palo Alto Networks, Fortinet.
System musi posiadać funkcjonalność „wstrzykiwania" poświadczeń do portali WEB poprzez wykorzystanie edytowalnych skryptów. Dopuszczalne jest wykorzystanie w tym celu funkcjonalności serwera usług terminalowych.
System musi posiadać funkcjonalność „wstrzykiwania" poświadczeń do aplikacji ("grubych klientów") poprzez wykorzystanie edytowalnych skryptów. Dopuszczalne jest wykorzystanie w tym celu funkcjonalności serwera usług terminalowych.

4. Zarządzanie hasłami (sejf haseł, generowanie i zmiana haseł na koncie):
System musi zapewniać definiowanie polityk złożoności hasła.
Polityki złożoności hasła muszą umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i wielkie litery, cyfry, znaki specjalne).
System musi generowaćć automatycznie hasła kont systemów docelowych w sposób pseudolosowy zgodnie ze zdefiniowaną polityką złożoności hasła.
System musi generować unikatowe hasła dla kont systemów docelowych.
System musi umożliwiać ręczną (inicjowaną przez administratora) zmianę hasła na wskazanym koncie systemu docelowego.
System musi umożliwiać zdefiniowanie polityk częstotliwości zmiany hasła na kontach systemów docelowych.
System musi zapewniać automatyczną zmianę hasła na wskazanych kontach systemów docelowych zgodnie ze zdefiniowaną polityką częstotliwości zmiany hasła.
System musi zapewniać walidację zgodności hasła na koncie systemu docelowego z hasłem zapisanym w systemie PAM.
Mechanizm automatycznej zmiany hasła pozwala na ponawianie próby zmiany hasła w przypadku nieudanej zmiany hasła przez system PAM na wskazanym koncie systemu docelowego lub w przypadku stwierdzenia niezgodności hasła na koncie systemu docelowego z hasłem zapisanym w systemie PAM.
System musi umożliwiać przeglądanie wcześniejszych wersji haseł dla zarządzanych kont.
System musi zapewniać funkcjonalności hasła „jednokrotnego użytku" polegającą na zmianie hasła na koncie systemu docelowego po zwolnieniu dostępu do danego konta.

5. Zarządzanie kluczami:
System musi umożliwiać zdefiniowanie reguł określających typ klucza, długość klucza, passphrase.
System musi umożliwiać automatyczne generowanie kluczy zgodnie ze zdefiniowanymi regułami.
System musi umożliwiać zdefiniowanie polityk częstotliwości zmiany kluczy systemów docelowych.

6. Zarządzanie sesjami:
System musi zapewniać transparentne zestawienie sesji do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.
System musi zapewniać zestawienie sesji do systemu docelowego z wykorzystaniem protokołów: SSH, RDP.
System musi zapewniać blokowanie i zrywanie sesji zestawionych do systemu docelowego przez system PAM przez uprawnionego operatora (audytora) .

System musi zapewniać zestawienie transparentne sesji SSH do systemu docelowegoz wykorzystaniem dowolnego klienta SSH, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.
System musi zapewniać zestawienie transparentne sesji RDP do systemu docelowego z wykorzystaniem dowolnego klienta RDP, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.
System musi umożliwiać zestawienie zarządzanego połączenia RDP/SSH z wykorzystaniem dowolnego klienta bez konieczności logowania się do portalu WEB systemu PAM.
System musi umożliwia skonfigurowanie liczników odliczających upływ czasu do zakończenia aktywnej sesji RDP oraz SSH.
System musi posiadać funkcjonalność wylogowania wykorzystywanego konta uprzywilejowanego w sesji RDP po upływie przydzielonego czasu.
System musi umożliwiać ustawienie limitu jednoczesnych sesji z wykorzystaniem określonego konta.

7. Monitorowanie i nagrywania sesji:
System musi zapewniać monitorowanie (podgląd) sesji zestawianych przez system PAM do systemów docelowych. Funkcjonalność ta dostępna jest tylko dla uprawnionych użytkowników systemu PAM.
System musi zapewniać nagrywanie sesji zestawianych przez system PAM do systemów docelowych.
System musi zapewniać odtwarzania sesji nagranych przez system PAM. Funkcjonalność ta dostępna jest tylko dla uprawnionych użytkowników systemu PAM.
System musi zapewniać rejestrację wydawanych komend i wyników działania komend dla sesji do systemów docelowych zestawianych przez system PAM z wykorzystaniem protokołu SSH do systemów docelowych. Sposób rejestracji umożliwia wyszukiwanie tekstowe.
System musi zapewniać rejestrację aktywności w sesji RDP, uwzględniającą wprowadzane ciągi znaków, kliknięcia myszą, nazwy otwieranych okien. Sposób rejestracji umożliwia wyszukiwanie tekstowe.
System nie może zezwalać na wykonanie eksportu składowanych w systemie nagrań do formatów video.

8. Zarządzanie użytkownikami i grupami:
System musi umożliwiać zarządzanie dostępem użytkowników systemu PAM do haseł i/lub sesji kont systemów docelowych.
System musi umożliwiać łączenie użytkowników systemu PAM w grupy w celu separacji uprawnień i uproszczenia procesu nadawania uprawnień.
System musi umożliwiać tworzenie grup lokalnych i domenowych z pełną synchronizacją z usługą katalogową klienta.

9. Wnioskowanie o dostęp do hasła i dostęp do hasła do, sesji:
System musi umożliwiać wnioskowanie o dostęp do hasła i/lub sesji, przy czym schemat akceptacji uwzględnia następujące modele: automatyczna akceptacja, akceptacja jednopoziomowa przez uprawnionego operatora, akceptacja jednopoziomowa przez wielu operatorów.
System musi umożliwiać wysyłanie powiadomienia email do użytkownika wnioskującego o dostęp do hasła i/lub sesji w przypadku zakończenia procesu zatwierdzania.
System musi umożliwiać określenie rodzaju dostępu jaki może uzyskać określony użytkownik (hasło do konta, nawiązanie sesji RDP/SSH, sesja aplikacyjna).

10. Raportowanie:
System musi zapewniać generowanie raportów automatyczne oraz „na żądanie".

System musi zapewniać ograniczenie dostępu do raportów dla wskazanej grupy administratorów i/lub użytkowników.
System musi zapewniać rejestrację i raportowanie procesu wnioskowania o dostęp do hasła i/lub sesji.
System musi zapewniać rejestracje i raportowanie każdej aktywności związanej z kontem uprzywilejowanym, a w szczególności zmianę hasła na koncie i pobranie hasła.
System musi zapewniać tworzenie nowych raportów z wykorzystaniem mechanizmu tabel przestawnych.

11. Integracja z innymi systemami (pełen zakres integracji opisany w dokumentacji):

System musi posiadać integrację (wbudowany connector) z systemami SIEM -Splunk, IBMQradar.
System musi posiadać integrację (wbudowany connector) z systemem IDM -SailPoint.
System musi posiadać integrację (wbudowany connector) z systemami ITSM– ServiceNow, Remedy, CA Service Desk Manager, Jira.
System musi umożliwiać wykorzystanie API pozwalającego na realizację podstawowych funkcjonalności systemu PAM.
System musi posiadać funkcjonalność wysyłania zdarzeń systemowych (syslog).

12. Wbudowany skaner zasobów:

System musi posiadać wbudowany skaner zasobów, umożliwiający wykonanie szczegółowego skanu (informacje dot. kont, portów, procesów, usług, oprogramowania, użytkowników).
System musi posiadać mechanizm automatycznego poddawania pod zarządzanie systemu PAM wykrytych kont uprzywilejowanych w przeskanowanych systemach.

13. Import danych:

System musi umożliwiać przeprowadzenie importu danych o zasobach wraz z informacją o kontach poprzez plik XML