Załącznik nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **dostawa wraz z wdrożeniem systemu zarządzania dostępem uprzywilejowanym.**
2. Opis wymagań technicznych Systemu zarządzania dostępem uprzywilejowanym przedstawione zostały poniżej:

L.p.	Opis wymagań technicznych
	Wymagania ogólne
1	Wymagane jest zaoferowanie licencji na System, uprawniających do: 1) zarządzania przez oferowane rozwiązanie systemami docelowymi Zamawiającego, w liczbie nie mniejszej niż 25. 2) korzystanie z oferowanego rozwiązania przez użytkowników w liczbie nie mniejszej niż 10, uzyskujących dostęp do systemów docelowych. W przypadku, jeśli oferowane rozwiązanie jest licencjonowane w ramach różnych modeli licencyjnych (np. per użytkownik albo per system), wówczas Wykonawca zaproponuje tylko jeden, wybrany model licencyjny.
2	Wymagane jest zapewnienie dla oferowanych licencji wsparcia producenta na warunkach oraz przez okres określone w umowie.
3	Wymagane jest zaoferowanie rozwiązania wraz z licencjami uprawniającymi do korzystania z wszystkich funkcjonalności określonych przez Zamawiającego oraz do jego działania w wymaganym przez Zamawiającego zakresie.
4	Wymagane jest, aby oferowane rozwiązanie spełniało wszystkie określone przez Zamawiającego wymagania minimalne, bez konieczności dokupowania dodatkowych elementów (np. urządzeń, modułów, licencji, itp.), nie będących przedmiotem zamówienia.
	Architektura
5	Dopuszcza się, aby oferowane rozwiązanie zostało dostarczone jako jeden z poniższych wariantów: 1) zamknięta platforma fizyczna (tzw. physical appliance), do implementacji w infrastrukturze Zamawiającego, przez którą należy rozumieć specjalizowane rozwiązanie, mające postać fizycznego urządzenia lub urządzeń, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja oraz pozostałe niezbędne do działania elementy), realizującego wszystkie wymagane funkcjonalności Systemu. W takim wypadku wymagane jest, aby: a. oferowany physical appliance istniał w liniach produktowych producenta Systemu;w ramach pojedynczego sprzętu była zapewniona redundancja co najmniej na poziomie zasilania oraz dysków wewnętrznych; b. sprzęt został zaoferowany wraz z niezbędnymi do instalacji w szafie szynami montażowymi lub uchwytami oraz niezbędnym okablowaniem; c. łączna wysokość sprzętu w ramach pojedynczej platformy fizycznej była nie większa niż 4U (jednostka wysokości szafy montażowej); d. była możliwość instalacji sprzętu w standardowej szafie typu rack 19” dowolnego producenta; 2) zamknięta platforma wirtualna (tzw. virtual appliance) do implementacji w ramach posiadanego przez Zamawiającego wirtualnego środowiska VM-Ware vSphere 6.x),

	przez którą należy rozumieć specjalizowane rozwiązanie, mające postać maszyny albo maszyn wirtualnych, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja oraz pozostałe niezbędne do działania elementy), realizujące funkcjonalności systemu PAM. W takim wypadku wymagane jest, aby oferowany virtual appliance istniał w liniach produktowych producenta Systemu; 3) oprogramowanie, do zainstalowania na zapewnionej przez Zamawiającego maszynie lub maszynach wirtualnych VM-Ware vSphere 6.x.
6	System PAM musi zapewnić możliwość wykonania i odtworzenia całości i/lub części Systemu PAM z kopii bezpieczeństwa w przypadku awarii (Disaster Recovery).
7	Interfejs użytkownika Systemu musi być dostępny przez przeglądarkę co najmniej jedną z następujących przeglądarek internetowych: Microsoft Internet Explorer, Google Chrome, Mozilla Firefox. Zarządzanie Systemem musi być realizowane za pomocą szyfrowanego protokołu HTTPS.
Uwierzytelnianie, autoryzacja i separacja uprawnień	
8	Musi być zapewnione logowanie do Systemu za pomocą kont lokalnych w Systemie PAM.
9	System PAM musi zapewnić integrację kont użytkowników Systemu PAM z mechanizmami uwierzytelniania Active Directory.
10	System PAM musi zapewnić możliwość integracji kont użytkowników Systemu PAM z mechanizmami autoryzacji w oparciu o grupy Active Directory.
11	System PAM musi zapewnić możliwość dwuskładnikowego uwierzytelniania.
12	System PAM musi zapewnić możliwość ograniczenia dostępu użytkowników do wybranych kont systemów docelowych.
13	System PAM musi zapewnić możliwość delegowania uprawnień do zarządzania wybranymi kontami systemów docelowych do wskazanego administratora, przy czym System PAM musi zapewnić utworzenie co najmniej 8 kont administratorów.
14	System PAM musi zapewnić możliwość oddzielenia ról typu: użytkownik (operator lub administrator danego systemu docelowego), administrator (zarządzający dostępem do danej grupy kont systemów docelowych), audytor (uprawniony do monitoringu i przeglądania sesji).
15	System PAM musi zapewnić możliwość ograniczenia dostępu (podglądu) do haseł kont systemów docelowych dla administratora systemu PAM.
Poufność i integralność	
16	System PAM musi zapewniać szyfrowaną komunikację pomiędzy wszystkimi elementami systemu.
17	System PAM musi zapewniać szyfrowanie haseł systemów Zamawiającego przechowywanych przez System PAM, przy czym siła szyfrowania musi być na poziomie AES-256 lub wyższym.
18	System PAM musi zapewniać szyfrowanie kopii bezpieczeństwa Systemu, przy czym siła szyfrowania musi być na poziomie AES-256 lub wyższym.
Zarządzanie sesjami	
19	System PAM musi zapewniać zestawienie sesji do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego dla posiadanych przez Zamawiającego systemów Windows, Unix, Linux, MS SQL i Cisco.
20	Musi być zapewnione zarządzanie dostępem użytkowników Systemu PAM do kont i sesji systemów docelowych.
21	System PAM musi zapewnić funkcjonalność automatycznej, zdefiniowanej przez administratora, podmiany loginu i hasła wprowadzonego przez użytkownika na inne hasło, istniejące na systemie docelowym.

22	System PAM musi zapewnić zestawienie sesji do systemu docelowego z wykorzystaniem protokołów: SSH, RDP, MySQL, TDS for MS SQL, HTTP, HTTPS.
23	System PAM musi zapewnić blokowanie i zrywanie sesji zestawionych do systemu docelowego przez system PAM.
24	System PAM musi zapewnić zestawienie sesji SSH do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego z wykorzystaniem klienta SSH używanego przez Zamawiającego (np. PuTTY, MobaXTerm).
25	System PAM musi zapewnić zestawienie transparentne sesji rdp do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego z wykorzystaniem klienta RDP używanego przez Zamawiającego.
Monitorowanie i nagrywania sesji	
26	System PAM musi zapewnić monitorowanie on-line (podgląd) sesji zestawianych przez system PAM do systemów docelowych. Funkcjonalność ta musi być dostępna dla wszystkich protokołów, o których mowa w pkt 22 powyżej, tylko dla uprawnionych użytkowników, administratorów i audytorów.
27	System PAM musi zapewnić nagrywania sesji zestawianych przez system PAM do systemów docelowych.
28	System PAM musi zapewnić wskazywanie dla których sesji ma być włączone nagrywanie.
29	System PAM musi zapewnić odtwarzania sesji nagranych przez system PAM. Funkcjonalność ta musi być dostępna tylko dla uprawnionych użytkowników, administratorów i audytorów. Zamawiający nie dopuszcza przesyłania tych danych do wizualnego przygotowania lub analizy poza Systemem, w szczególności do chmury.
30	System PAM musi zapewnić rejestrację wydawanych komend i wyników działania komend dla sesji zestawianych przez system PAM z wykorzystaniem protokołu ssh do systemów docelowych. Sposób rejestracji musi zapewnić możliwość wyszukiwania tekstowego.
31	System PAM musi zapewnić automatyczne, bieżące i ciągłe blokowanie niepożądanych komend i funkcji wpisanych z klawiatury jeszcze przed ich wykonaniem w systemie docelowym, wraz z możliwym do zdefiniowania równoczesnym automatycznym wysłaniem powiadomienia do zdefiniowanych w systemie osób odpowiedzialnych za nadzór, za pomocą poczty elektronicznej.
32	System PAM musi posiadać funkcjonalność predefiniowania listy komend i funkcji niepożądanych, która musi być w pełni edytowalna, tj. musi zapewniać możliwość dodawania, odejmowania, modyfikacji pozycji w dowolnej chwili, ze skutkiem dla sesji nawiązywanych po zdefiniowaniu ww. listy komend i funkcji.
33	System PAM musi zapewnić definiowanie polityk retencji nagranych sesji na poziomie co najmniej 2 lat.
Wnioskowanie o dostęp i dostęp do hasła, sesji	
34	System PAM musi zapewnić wnioskowanie o dostęp do sesji, przy czym schemat akceptacji musi uwzględniać minimum następujące modele: automatyczna akceptacja, akceptacja jednopoziomowa przez administratora danej grupy kont systemów docelowych, akceptacja jednopoziomowa przez wielu administratorów danej grupy kont systemów docelowych.
35	System PAM musi zapewnić wysłanie powiadomienia email do użytkownika wnioskującego o dostęp do sesji w przypadku zakończenia procesu zatwierdzania.
36	System PAM musi zapewnić pobranie tego samego hasła do konta przez więcej niż jednego użytkownika.
37	System PAM musi zapewnić skopiowanie pobranego hasła do schowka.
Auditing i raportowanie	

38	System PAM musi zapewnić automatyczne i „na żądanie” generowanie raportów.
39	System PAM musi zapewnić generowanie raportów w formacie CSV.
40	System PAM musi zapewnić ograniczenie dostępu do raportów dla wskazanej grupy administratorów i użytkowników.
41	System PAM musi zapewnić rejestrację i raportowanie procesu wnioskowania o dostęp do hasła i/lub sesji.
42	System PAM musi zapewnić rejestracje i raportowanie każdej aktywności związanej z kontem uprzywilejowanym, a w szczególności zmianę hasła na koncie i pobranie hasła.
43	System PAM musi zapewnić rejestrację i raportowanie działań wykonywanych przez administratorów Systemu PAM.

3. W ramach zamówienia Wykonawca zobowiązany jest do przeprowadzenia szkoleń, dla czterech pracowników Zamawiającego, na warunkach opisanych w § 5 Umowy.