**Procedura konkursowa nr: 05 Z PK 22**

 Załącznik nr **1** do Zaproszenia

…………..............................

 (pieczęć firmowa Wykonawcy)

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**DOSTAWA SYSTEMU KONTROLI DOSTĘPU ADMINISTRACYJNEGO WRAZ Z WDROŻENIEM
(CPV: 48200000-0, 48900000-7)**

Przedmiotem zamówienia jest dostawa systemu kontroli dostępu administracyjnego wraz z wdrożeniem. Dostarczony system ma zapewnić podniesienie poziomu cyberbezpieczeństwa systemów teleinformatycznych w Kujawsko-Pomorskim Centrum Pulmonologii w Bydgoszczy..

* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta (jeśli podlega certyfikacji).
1. Instalacja oraz konfiguracji oprogramowania.
2. Testy rozwiązania dla minimum 1 wdrożonej kontrolowanej sesji, poprzez udział zewnętrznego kontraktora lub symulacji zewnętrznego kontraktora przez pracownika Zamawiającego
3. Szkolenie stanowiskowe dla administratorów demonstrujący sposób zarządzania systemem, obsługę kontrolowanej sesji, sposoby zakańczania kontrolowanych sesji, dołączanie do sesji, konfigurację nowej sesji, usuwanie skonfigurowanej sesji obsługę logów, nagrań sesji. Celem szkolenia jest uzyskanie, przez administratorów Zamawiającego, poziomu wiedzy umożliwiającego samodzielne zarządzanie systemem.
4. Dostarczenie dokumentacji powykonawczej dostarczonego systemu, która będzie składała się co najmniej z następujących elementów:
	* Procedur administracyjnych,
	* Opisu konfiguracji sesji wykonanych w ramach wdrożenia,
	* Schematu blokowego, logicznego wraz adresacją IP
	* Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją
	* Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,
	* Zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni.
	* Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

**Opis parametrów minimalnych dostarczanego oprogramowania:**

Zamawiający wymaga, aby Wykonawca spełniał wymagania w zakresie:

Licencje muszą mieć charakter bezterminowy. Działanie systemu nie może wymagać dodatkowych opłat, po wygaśnięciu gwarancji producenta. Zakończenie gwarancji może jedynie oznaczać: brak dostępu do aktualizacji oprogramowania, brak nieodpłatnego usuwania błędów oraz brak pomocy technicznej.

Nieodpłatna gwarancja producenta o czasie trwania minimum 12 miesięcy.

Zamawiający wymaga dostarczenia systemu obsługującego nie mniej niż 20 nadzorowanych sesji administracyjnych rozumianych jako unikalne usługi sieciowe na serwerze.

**Warunki gwarancji**

Możliwość zgłoszenia błędu w oprogramowaniu w dni robocze, dostęp do systemu obsługi zgłoszeń serwisowych www, e-mail, dostęp do nowych wersji oprogramowania, poprawki oprogramowania

Usuwanie błędów

● Błąd Krytyczny – w ciągu 6 godzin

Definicja błędu krytycznego: Brak poprawnego działania środowiska produkcyjnego, praca nie może być kontynuowana, operacje krytyczne dla procesu biznesowego są niemożliwe. Kluczowa funkcjonalność nie działa.

● Błąd Niekrytyczny – następny dzień roboczy

Definicja błędu niekrytycznego: Utrudnienia w działaniu w środowisku produkcyjnym w zakresie kluczowej funkcjonalności, brak działania w zakresie pozostałej funkcjonalności.

● Usterka – trzeci dzień roboczy

Definicja Usterki: Wszelkie błędy nie będące błędami krytycznymi oraz niekrytycznymi

**Architektura**

1. System musi być dostarczany w formie 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. Zamawiający posiada platformę wirtualizacyjną Vmware.
2. System musi być zaprojektowany i przygotowany do umieszczenia w DMZ (hardening producenta) lub sieci wewnętrznej LAN.
3. Jeżeli system jest umieszczony w DMZ, na potrzeby realizacji swoich funkcji nie może wymagać zestawienia tunelu VPN pomiędzy siecią LAN organizacji, a komputerem nawiązującego sesję. Nie może też wykorzystywać technologii chmurowej do nawiązania połączenia.
4. System musi umożliwiać rozbudowę do trybu pracy awaryjnej (klaster HA) zapewniający synchronizację danych między dwoma urządzeniami do uprzywilejowanego dostępu zdalnego. Uproszczony proces przełączenia maszyny niedostępnej na dostępną musi odbywać się w sposób automatyczny.
5. Serwery proxy (nawiązywanie sesji w sposób bezagentowy) muszą być zarządzane w sposób centralny z poziomu oprogramowania do uprzywilejowanego dostępu zdalnego (konfiguracja minimalnie w zakresie: nadawania uprawnień dostępowych do serwera proxy dla sesji uprzywilejowanych, utworzenie serwera proxy, wyłączenie serwera proxy, utworzenie klastra wysokiej dostępności).
6. Komunikacja między elementami systemu do uprzywilejowanego dostępu zdalnego (tj. oprogramowaniem uprzywilejowanego dostępu zdalnego, oraz serwerami proxy) musi być szyfrowana (TLS lub RDS Security) i odbywać się na jednym porcie 443.
7. System musi posiadać wsparcie dla protokołów SSH, RDP oraz VNC.
8. System musi posiadać możliwość rozbudowy o moduł obsługi sesji do aplikacji WEB (wbudowana przeglądarka WWW).
9. System musi posiadać możliwość uruchomienia sesji aplikacyjnych (uruchomienie wskazanej aplikacji z serwera usług terminalowych lub uruchomienie aplikacji za pomocą dedykowanego agenta).
10. System musi posiadać możliwość tunelowania protokołów TCP na zdefiniowanym porcie między komputerem nawiązującego sesje, a zarządzanym systemem.
11. System ma być dostarczony w polskiej wersji językowej (zarówno menu konfiguracyjne systemu jak i interfejs klientów za pomocą których realizowane są sesje).

**Funkcje operacyjne sytemu uprzywilejowanego dostępu zdalnego**

1. Logowanie do systemu uprzywilejowanego dostępu zdalnego musi odbywać się poprzez konta lokalne (tworzone na poziomie systemu do uprzywilejowanego dostępu zdalnego) lub konta i grupy importowane z Active Directory.
2. Proces autentykacji przy logowaniu do systemu uprzywilejowanego dostępu zdalnego musi być zabezpieczony drugim składnikiem (2FA).
3. System musi realizować następujące scenariusze nawiązywania sesji:
	1. za pomocą klienta zainstalowanego na komputerze nawiązującego sesję (gruby klient),
	2. za pomocą przeglądarki WWW z komputera nawiązującego sesję (bez potrzeby instalacji klienta),
	3. za pomocą klienta zainstalowanego na urządzeniu mobilnym (minimum wsparcie dla systemu Android).
4. System musi umożliwiać opcję zastosowania własnych klientów RDP i SSH.
5. System musi umożliwiać realizację sesji do stacji roboczych (przynajmniej Windows i Linux) i współdzielenie tej samej sesji między pełniącym funkcję administratora systemu, a operatorem pracującym przy stacji roboczej (funkcja wsparcia zdalnego).
6. Rozpoczęcie sesji współdzielonej między pełniącym funkcję administratora systemu, a operatorem stacji roboczej musi podlegać procesowi akceptacji przez operatora stacji roboczej do której realizowana jest ta sesja.
7. Rozpoczęcie sesji uprzywilejowanej musi podlegać kontroli dostępu poprzez:
	1. Wysyłanie powiadomień o zdarzeniu rozpoczęcia i zakończenia sesji uprzywilejowanej do zdefiniowanej listy osób,
	2. Ograniczenie możliwości nawiązywania sesji uprzywilejowanej do określonych dni i godzin, oraz do określonych grup zasobów.
	3. Włącznie procesu wnioskowania o dostęp do zasobów i mechanizmu akceptacji lub odrzucenia wniosku przez właściciela zasobu. We wniosku muszą znaleźć się przynajmniej zakres dat, kiedy będzie nawiązywana sesja oraz pole pozwalające opisać zakres wykonywanych przez prac. Wniosek musi być wysyłany w celu akceptacji do zdefiniowanej listy osób.
	4. Ograniczenie adresów IP / lub adresów sieci, z których można wykonywać połączenia.
8. Konsola dostępowa musi posiadać co najmniej poniższe funkcje:
	1. widok grup zasobów z możliwością nawiązania sesji do tych zasobów (za pomocą menu kontekstowego lub podwójnego kliknięcia), oraz możliwością wyszukiwania zasobów po ciągach znaków,
	2. szczegółowy opis zasobu, do którego możliwe jest nawiązanie sesji, zawierający nazwę hosta / adres IP, status (aktywny/nieaktywny), typ systemu operacyjnego, edytowalną nazwę skróconą.
9. System musi umożliwić wyłączenie synchronizacji schowka i kopiowania plików między komputerem nawiązującego sesję a zarządzanym zasobem.
10. System w trakcie trwania sesji musi umożliwiać:
	1. Dołączenie do sesji dodatkowych użytkowników posiadających konta w systemie uprzywilejowanego dostępu zdalnego;
	2. Dołączenie dodatkowych użytkowników do sesji, nieposiadających konta w systemie uprzywilejowanego dostępu zdalnego przy jednoczesnej możliwości nałożenia dodatkowych restrykcji dla takiej osoby (minimum w zakresie odebrania kontroli myszy i klawiatury, automatyczne zakończenie sesji w przypadku, gdy połączenie autoryzowanego użytkownika ulegnie awarii);
	3. Przejęcie sesji przez uprawnioną osobę (audytora) i jej zakończenie.

**Funkcje raportowania**

1. System musi posiadać wbudowany i centralnie zarządzany moduł raportowy.
2. System musi generować centralnie konfigurowane i składowane raporty z przeprowadzonych sesji (łącznie z nagraniami sesji).
3. System musi rejestrować sesje graficzne oraz sesje z wierszem poleceń.
4. System musi umożliwiać wybór rozdzielczości rejestrowanych sesji.
5. W systemie muszą być dostępne raporty dotyczące co najmniej przeprowadzonych sesji i wykorzystania poświadczeń z wbudowanego magazynu haseł.
6. Raporty dotyczące przeprowadzonych sesji muszą podlegać filtrowaniu co najmniej (wymagane wszystkie wymienione) w zakresie daty, nazwy użytkownika (nawiązującego sesję), nazwy / adresu IP zarządzanego zasobu, grupy zarządzanych zasobów.
7. W szczegółach raportu sesji muszą znajdować się co najmniej informacje na temat:
	1. daty rozpoczęcia i zakończenia sesji (długość trwania sesji),
	2. nazwy konta przechowywanego we wbudowanym magazynie haseł za pomocą którego zalogowano się do systemu,
	3. nagrania z sesji (sesje graficzne oraz okna konsoli),
	4. wszystkich uczestników sesji (osoby, które dołączały do sesji w trakcie jej trwania),
	5. listy zdarzeń (log) dotyczący pracy narzędzia uprzywilejowanego dostępu zdalnego,

**Wbudowany magazyn haseł**

1. System musi posiadać wbudowaną funkcjonalność magazynu poświadczeń (przechowywanie nazw kont i haseł, ukrywanie widoczności haseł przed nawiązującym sesję).
2. System musi umożliwiać dodawanie kont wykorzystywanych do zdalnego logowania co najmniej poprzez:
	1. wprowadzenie ręczne z poziomu interfejsu konfiguracyjnego narzędzia,
	2. wyszukanie i import z Active Directory, z możliwością automatycznej zmiany haseł na takich kontach.
	3. możliwość zintegrowania pobierania poświadczeń z systemu PAM (przynajmniej jednego),
	4. poświadczenia muszą być prezentowane w kontekście zasobu do którego łączy się użytkownik (przy nawiązywaniu sesji musi być możliwość wyboru poświadczeń występujących wyłącznie na danym zasobie).
3. Użycie poświadczeń przez nawiązującego sesję użytkownika musi podlegać kontroli dostępu. Uprawnienia do korzystania z danych poświadczeń (haseł) muszą być przyznawane dla pojedynczego konta dostawcy lub dla grupy kont dostawców.
4. Hasła przechowywane w magazynie haseł muszą być szyfrowane AES256 lub lepszym.

**Integracje**

1. System musi posiadać otwarte API w zakresie pozwalającym na wykonanie integracji z oprogramowaniem firm trzecich.
2. System musi umożliwiać wykonanie integracji z systemami typu SIEM (syslog).
3. System musi umożliwiać wykonanie integracji z systemem PAM w zakresie pobierania z niego poświadczeń.
4. System musi umożliwiać wysyłanie powiadomień z wykorzystaniem SMTP.

**Kontrola dostępu**

1. System musi posiadać możliwość zdefiniowania restrykcji sieciowych pozwalających ograniczyć dostęp do interfejsu zarządzającego oprogramowaniem przynajmniej w zakresie zdefiniowania adresów IP hostów lub adresów sieci znajdujących się na białej liście (liście dostępowej) i domyślnej akcji odrzucania innego ruchu skierowanego do interfejsu zarządzającego.
2. System musi umożliwiać edycję poziomu uprawnień użytkowników lub grup użytkowników co najmniej w zakresie:
	1. edycji grup zasobów w zakresie nadawania uprawnień dostępowych do zasobów dla użytkownika nawiązującego sesję oraz uprawnień do edycji tych zasobów (zabronienie możliwości edycji zasobów w systemie uprzywilejowanego dostępu zdalnego),
	2. edycji i tworzenia nowych poświadczeń w magazynie haseł oraz do przyznawania uprawnień dla nawiązującego sesję do możliwości wykorzystania tych poświadczeń,
	3. generowania i podglądu raportów w tym nagrań z sesji,
	4. możliwości zapraszania do sesji dodatkowych użytkowników,
	5. możliwości odebrania lub nadania uprawnień do realizowania sesji.

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

 (podpis/y i pieczęcie Wykonawcy)