Załącznik nr 1

OFERTA

<table>
<tr><td>Zamawiający:</td><td colspan="4">Uniwersytet Śląski w Katowicach
ul. Bankowa 12
40-007 Katowice</td></tr>
<tr><td>Nazwa (firma) / imię i nazwisko Wykonawcy / Wykonawców wspólnie ubiegających się o zamówienie:</td><td colspan="4"></td></tr>
<tr><td rowspan="3">Adres Wykonawcy:</td><td>Ulica, nr domu / nr lokalu:</td><td colspan="3"></td></tr>
<tr><td>Miejscowość i kod pocztowy:</td><td colspan="3"></td></tr>
<tr><td>Województwo:</td><td></td><td>Kraj:</td><td></td></tr>
<tr><td>NIP:</td><td></td><td>REGON:</td><td colspan="2"></td></tr>
<tr><td>Wysokość kapitału zakładowego:
(dot. Sp. z o.o.)</td><td></td><td>Wysokość kapitału wpłaconego:
(dot. S.A.)</td><td colspan="2"></td></tr>
<tr><td>Adres do korespondencji:
(jeżeli jest inny niż podany powyżej)</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Osoba upoważniona do kontaktu z Zamawiającym:</td><td colspan="2" rowspan="2"></td><td>Telefon:</td><td></td></tr>
<tr><td>e-mail:</td><td></td></tr>
</table>

Odpowiadając na publiczne ogłoszenie o zamówieniu w postępowaniu

nr **122626/2019**

prowadzonego z wyłączeniem przepisów ustawy – Prawo zamówień publicznych p.n.:

„Dostawa Systemu bezpieczeństwa kont uprzywilejowanych z możliwością nagrywania sesji oraz dostawa Systemu do audytowania zmian i powiadamiania w rozproszonym środowisku Active Directory na potrzeby Działu Informatycznych Systemów Zarządzania”

składamy następującą ofertę:

1. Oferujemy realizację przedmiotu zamówienia zgodnie z warunkami i na zasadach zawartych w Ogłoszeniu o zamiarze udzielenia zamówienia za łącznym wynagrodzeniem:

Cena netto: ……..…… …PLN	Słownie: …… ……...PLN
Stawka podatku VAT: …… ……..%	Doliczona wartość podatku VAT: ……..... PLN
Cena oferty brutto: …… ……PLN	Słownie: ……..……..…… ……PLN

Wyżej podana cena stanowi cenę w rozumieniu art. 3 ust. 1 pkt 1 i ust. 2 ustawy z dnia 9 maja 2014r. o informowaniu o cenach towarów i usług (Dz. U. poz. 915), a więc wartość wyrażoną w jednostkach pieniężnych, którą kupujący jest obowiązany zapłacić przedsiębiorcy za towar lub usługę. Zgodnie z przepisem art. 3 ust. 2 ustawy o informowaniu o cenach

towarów i usług, w cenie uwzględnia się podatek od towarów i usług oraz podatek akcyzowy, jeżeli na podstawie odrębnych przepisów sprzedaż towaru (usługi) podlega obciążeniu podatkiem od towarów i usług lub podatkiem akcyzowym. Przez cenę rozumie się również stawkę taryfową.

Oświadczamy, iż zaoferowana cena zawiera wszelkie koszty poniesione w celu należytego wykonania przedmiotu umowy, zgodnie z postanowieniami Ogłoszenia o zamiarze udzielenia zamówienia oraz koszty ogólne, wszelkie podatki i opłaty, elementy ryzyka związane z realizacją zamówienia, zysk Wykonawcy. Cena zawiera koszty związane ze sprzedażą oraz dostarczeniem i wdrożeniem przedmiotu zamówienia.

Oferujemy realizację przedmiotu zamówienia za ww. cenę zgodnie z poniższym zestawieniem:

L.P.	**NAZWA OPROGRAMOWANIA** Minimalne parametry wymagane przez Zamawiającego	**Liczba sztuk**	**OPIS TECHNICZNY OFEROWANEGO SPRZĘTU** Należy wskazać wszystkie elementy składowe oferowanego sprzętu w odniesieniu do kolumny z lewej strony	**Cena netto**
1.	**Przedmiotem zamówienia jest zakup Systemu bezpieczeństwa kont uprzywilejowanych z możliwością nagrywania sesji na potrzeby Działu Informatycznych Systemów Zarządzania z siedzibą w Katowicach przy ul. Bankowej 12** Przedmiotem zamówienia jest: 1. Dostarczenie licencji na oprogramowanie dla min. 100 użytkowników, 1000 zasobów, licencja ta ma zawierać konta do zarządzania użytkownikami i zasobami ilości nie mniejszej niż 5. 2. Instalacja oprogramowania wraz z dwudniowymi warsztatami z zakresu administracji systemem dla nie więcej niż 5 użytkowników 3. Wsparcie oraz pomoc techniczną producenta przez okrese jednego roku obejmującą: - dostęp do poprawek i nowych wersji oprogramowania - dostęp do bazy wiedzy i portalu pomocy technicznej w języku polskim - obsługę zgłoszeń wysyłanych za pomocą poczty elektronicznej i telefonu, oraz za pomocą portalu serwisowego w języku polskim **<u>Wymagania podstawowe oprogramowania:</u>** • Dostęp do systemu dla wszystkich użytkowników ma	**1**		

	być zapewniony za pośrednictwem szyfrowanej strony internetowej w języku polskim i angielskim. • System musi posiadać centralne repozytorium haseł i przechowywać je w odpowiednio zabezpieczony sposób. Cechy repozytorium haseł: o definiowanie właścicieli haseł o domyślnie administrator dodający hasło musi zostać jego właścicielem o właściciel musi mieć możliwość przydzielania poziomów uprawnień o w przypadku opuszczenia organizacji przez administratora system musi zapewniać możliwość transferu własności na innego administratora • System musi umożliwiać ograniczony dostęp do zasobów przydzielanych w według potrzeby. Cechy mechanizmu przydzielania zasobów: o musi zapewniać dostęp tylko i wyłącznie do przewidzianych dla użytkownika zasobów o ma posiadać zestaw predefiniowanych ról dla administratorów i użytkowników administrator może przeglądać jedynie te zasoby i hasła, które zostały samodzielnie stworzone przez niego lub udostępnione jemu przez innych użytkowników o administrator haseł ma mieć możliwość wykonywania wszystkich dostępnych operacji na zasobach bez możliwości konfiguracji i zarządzania systemem. o Administrator haseł może przeglądać jedynie te zasoby i hasła, które zostały samodzielnie stworzone przez niego lub udostępnione jemu			

	przez innych użytkowników ○ administrator / administrator haseł może mieć status „super administratora" przydzielony przez innego administratora (statusu tego nie może przydzielić sam sobie). "super administrator" posiada uprawnienia zarządzania wszystkimi zasobami dodanymi do system zarządzania hasłami przez wszystkich administratorów i użytkowników. ○ użytkownicy haseł mogą jedynie przeglądać hasła im przydzielone przez administratora lub administratora haseł ○ użytkownicy haseł mogą modyfikować hasła jeżeli uprawnienia współdzielenia zezwalają im na to ○ audytorzy haseł muszą mieć te same uprawnienia co użytkownicy haseł i dodatkowo muszą mieć dostęp do raportów i audytu rekordów • System musi umożliwiać szyfrowanie nazw użytkowników i haseł algorytmem AES (Advanced Encryption Standard). Szczegółowe opcje zabezpieczeń: ○ szyfrowane nazwy użytkowników i hasła muszą być bezpiecznie składowane w bazie danych systemu funkcjonującej jako centralne repozytorium. ○ system musi zapewniać funkcjonalność przypisywania własności do zasobów, kont użytkowników i haseł. ○ zasoby posiadane przez administratora lub innego użytkownika nie mogą być przeglądane			

	przez innych użytkowników chyba że są one udostępniane o system musi umożliwiać pełen transfer uprawnień na innego administratora. o system musi umożliwiać przydzielanie pozwoleń dla innych użytkowników na przegląd / edycję / zarządzanie hasłami podczas gdy jeden administrator dalej pozostaje właścicielem • System musi posiadać funkcjonalność zarządzania hasłami współdzielonymi. Cechy zasobów współdzielonych: o możliwość śledzenie kont użytkowników a nie jedynie ról o zapewnienie dostępu do określonych zasobów tylko i wyłącznie dla autoryzowanych użytkowników haseł administracyjnych • System musi umożliwiać zarządzanie dostępem aplikacja – aplikacja i aplikacja – baza danych. Cechy zarządzania dostępem: o możliwość zarządzania dostępem do aplikacji lub baz danych za pośrednictwem innych aplikacji, w których zakodowany jest dostęp do tych aplikacji / baz danych o zapewnienie wydajnego mechanizmu eliminowania zakodowanych haseł poprzez odpytanie systemu zarządzania hasłami bez konieczności interwencji użytkownika. o ma posiadać moduł API (Application Programming Interface), którego wykorzystanie zapewnia programowalne wykonanie zapytań przez aplikacje lub skrypty			

	o pozyskanie hasła z systemu zarządzania hasłami by nawiązać połączenie z inną aplikacją lub bazą danych. o Na potrzeby funkcjonalności system musi udostępniać co najmniej dwie metody API- API w oparciu o XML-RPC po HTTPS, - XML-RPC API musi posiadać wbudowane API do klasy opakowującej, umożliwiające integrację systemu zarządzania hasłami z aplikacjami Java • System musi umożliwiać integrację z systemem Windows Active Directory (AD) lub innymi usługami LDAP. W szczególności: o system musi umożliwiać logowanie do system zarządzania hasłami za pośrednictwem usług katalogowych AD/LDAP o musi uwzględniać restrykcje uwierzytelniania AD/LDAP podczas logowania o Administrator systemu zarządzania hasłami musi mieć możliwość importowania użytkowników i grup użytkowników z AD/LDAP do systemu o Jeżeli nowy użytkownik pojawia się w AD/LDAP, istnieje możliwość automatycznego dodania takiego użytkownika do systemu • System musi zapewniać funkcje ciągu zadań kontroli dostępu do haseł. Cechy: o musi zapewniać dodatkowy poziom weryfikacji dostępu do zasobów o musi umożliwiać przydzielanie dostępu tymczasowego o ramach procedur musi umożliwiać przydzielanie dostępu wyłącznego w			

	określonym czasie o w przypadku kolejki żądań uruchamia proces kolejkowania o jeżeli administrator nie zaakceptuje zapytania w określonym czasie lub zaneguje zapytanie, zapytanie zostaje unieważnione o możliwość akceptacji przez dwóch administratorów – tylko akceptacja obu udziela dostępu o w sytuacji w której inny użytkownik wymaga dostępu do hasła w tym samym czasie uzyska on dostęp po wcześniejszym zwolnieniu hasła przez poprzedniego użytkownika. Reguła ta musi dotyczyć również administratorów, administratorów haseł i właścicieli haseł. o administrator musi mieć możliwość wymuszenia dostępu do hasła w dowolnym czasie. W takiej sytuacji hasło musi zostać zwolnione blokując dostęp dla użytkowników o po wykonaniu prac przez użytkownika hasło zostaje zresetowane o musi zapewniać funkcje automatycznego logowania do zasobów z poziomu systemu zarządzania hasłami bez konieczności kopiowania haseł do zasobów docelowych, za pośrednictwem konsoli webowej. o System musi zapewniać co najmniej trzy metody automatycznego logowania: - brama automatycznego logowania - skrypt wspierający automatyczne logowanie dla aplikacji - logowanie do aplikacji webowych z wykorzystaniem linku. o System powinien umożliwiać zdalny reset haseł			

	dla systemów Windows, domeny Windows, systemów Linux, IBM AIX, HP UNIX, Solaris, Mac OS, MS SQ, MySQL, Oracle DB, Sybase ASE, urządzeń HP ProCurve i Cisco (IOS, CatOS, PIX). o Zdalny reset haseł musi być umożliwiony za pośrednictwem co najmniej dwóch metod: - agenta system zarządzania hasłami - w trybie bezagentowym - musi być wyposażony w notyfikację w przypadku uruchomienia procedury resetu haseł • System musi umożliwiać zdalne logowanie o system musi umożliwiać logowanie z poziomu dowolnej przeglądarki wspierającej protokół HTML w wersji 5 dla sesji Windows RDP, SSH i Telnet bez konieczności instalacji agentów o zdalne sesje muszą być tunelowane przez serwer centralny sytemu zarządzania hasłami bez konieczności bezpośredniej komunikacji urządzenia użytkownika z urządzeniem docelowym o zdalne sesje muszą dawać administratorowi możliwość śledzenia sesji, otwartej przez innego użytkownika, na żywo, tzw. Session shadowing o administrator ma mieć możliwość przerwania danej sesji użytkownika w dowolnym momencie • System musi umożliwiać nagrywanie sesji użytkowników uprzywilejowanych o sesje muszą mieć możliwość eksportu o sesje muszą mieć możliwość usuwania po			

	określonym czasie ○ sesje oraz wykonany chat podczas sesji muszą mieć możliwość wybiórczego usuwania • System musi generować powiadomienia ○ dla każdej operacjach na hasłach ○ z możliwością definiowania powiadomień email ○ z możliwością generowania pułapek SNMP lub rejestrów syslog i przesłania ich do systemów SIEM (Security Information and Event Management) ○ z możliwością generowania zdarzeń w ramach rejestrów syslog • System musi umożliwiać audyt operacji co najmniej w trzech kategoriach: Cechy audytu: ○ audyt zasobów – wszystkie operacje związane z zasobami, grupami zasobów, kontami, hasłami, udziałami i politykami ○ audyt użytkowników – wszystkie operacje wykonane w systemie zarządzania hasłami przez jego użytkowników ○ audyt zadań – rejestr zdefiniowanych zdań ○ odtwarzanie nagranych sesji • System musi umożliwiać dwupoziomowe uwierzytelnianie ○ oprócz podstawowego system uwierzytelniania (lokalne / AD / LDAP) system musi umożliwiać co najmniej jeden dodatkowy poziom uwierzytelniania: ○ możliwość weryfikacji przez telefon ○ jednorazowe hasło dostarczone przez email ○ jednorazowy token RSA SecureID a Token musi być zmieniany co najmniej co 6 sekund			

	• System musi funkcjonować w trybie wysokiej dostępności (High Availability)
	  ○ wszyscy użytkownicy rejestrują się do serwera głównego
	  ○ druga instancja serwera funkcjonuje jako serwer typu Secondary / Standby
	  ○ synchronizacja danych między serwerem głównym a Secondary/Standby musi następować w zabezpieczony sposób
	  ○ W dowolnym momencie czasu, w sytuacji awarii serwera głównego serwer Secondary/Standby przejmuje wszystkie funkcje serwera głównego
	• System musi posiadać możliwość włączenia dodatkowej kontroli dostępu do zasobów oraz ograniczenia możliwości łączenia zdalną sesją spoza systemu. Cechy ograniczeń systemu:
	  ○ musi posiadać możliwość włączenia i wyłączenia zatwierdzania dostępu
	  ○ musi posiadać możliwość wyłączenia podglądu haseł
	  ○ musi posiadać możliwość automatycznego resetowania haseł po każdej sesji
	• System musi posiadać zdefiniowane raporty oraz zabezpieczenia wspierające zgodność z RODO, w tym:
	  ○ możliwość zaciemniania danych osobowych w raportach
	  ○ kontroli numerów IP z jakich następuje połączenie z aplikacją zarówno sesji z przeglądarki internetowej jak i API.
	• System musi mieć możliwość natychmiastowego wyłączenia w przypadku sytuacji awaryjnej, w tym			

	wyłączenia wszelkiej komunikacji z agentami oraz po API.			
2.	**Przedmiotem zamówienia jest zakup Systemu do audytowania zmian i powiadamiania w rozproszonym środowisku Active Directory na potrzeby Działu Informatycznych Systemów Zarządzania z siedzibą w Katowicach przy ul. Bankowej 12** Przedmiotem zamówienia jest: 1. Dostarczenie licencji i oprogramowania dla trzech kontrolerów domeny i 3 serwerów plików 2. Wsparcie oraz pomoc techniczną producenta przez okres jednego roku obejmującą: - dostęp do poprawek i nowych wersji oprogramowania - dostęp do bazy wiedzy i portalu pomocy technicznej w języku polskim - obsługę zgłoszeń wysyłanych za pomocą poczty elektronicznej i telefonu, oraz za pomocą portalu serwisowego w języku polskim **<u>Wymagania podstawowe oprogramowania:</u>** • System musi umożliwiać audyt zdarzeń zarówno w czasie rzeczywistym jak i w ustawianych interwałach czasowych. • System ma mieć możliwość pracy bez instalacji agentów. • System musi umożliwiać zbiorcze audytowanie środowiska Active Directory, a w szczególności:	**1**		

	○ Nieudane próby zalogowania do środowiska domenowego na: stacjach roboczych, serwerach, kontrolerach domen ○ Poprawne logowanie użytkowników wraz z pełną historią logowania ○ Nieudane próby logowania na serwery Radius oraz historię logowań ○ Zmiany dokonywane na kontach użytkowników, a w szczególności: tworzenie kont, usuwanie kont, dezaktywacja kont, modyfikacja haseł, spis zablokowanych użytkowników, historia zmian na kontach użytkowników ○ Audyt zmian w grupie obiektów, w grupie bezpieczeństwa, operacje związane z tworzeniem i usuwaniem grup ○ Zmiany dokonane na obiektach komputerów, a w szczególności: tworzenie kont, usuwanie kont, dezaktywacja kont, historię kont ○ Audyt zmian w jednostkach organizacyjnych, a w szczególności: tworzenie OU, usuwanie OU, lista modyfikowanych OU, historia zmian OU ○ Audyt zmian w zasadach grupowych, a w szczególności: tworzenie GPO, usuwanie GPO, lista modyfikowanych GPO, historia zmian GPO, zaawansowane zmiany w GPO ○ Audyt zmian uprawnień, a w szczególności: - Uprawnienia dotyczące poziomu dostępu do domeny - Uprawnienia zmian OU - Uprawnienia zmian w kontenerach - Uprawnienia zmian w GPO - Uprawnienia zmian użytkowników			

	- Uprawnienia zmian grup - Uprawnienia zmian komputerów - Uprawnienia zmian DNS o Zmiany w DNS o Audyt zmian na serwerach plików, a w szczególności: Windows, Windows file Cluster, MC, NetApp • System musi umożliwiać budowanie własnych raportów wykorzystujących wbudowane funkcjonalności wraz z możliwością harmonogramowania: o Audyt wydruków o Raporty zgodności dla audytów, a w szczególności: SOX, HIPAA, PCI-DSS, GLBA, FISMA, RODO/GDPR • Audyt zmian na serwerach członkowskich • Audyt stacji roboczych • System musi posiadać moduł powiadomień w formie alertów: o Widocznych w systemie o Drogą mailową • System musi umożliwiać wykonanie różnego rodzaju skryptów, które pozwalają na natychmiastową reakcję na zagrożenie. • System posiada alerty o przekroczonej przestrzeni dyskowej • System musi umożliwiać zwolnienie zajętej przez siebie roboczej przestrzeni dyskowej • System przechowuje zarchiwizowany zbiór logów z audytowanego środowiska i posiada możliwość dokładnego ustawiania czasu przeniesienia do			

	archiwum. • System musi umożliwiać audyt Azure Active Directory, a w szczególności: o Poprawne logowanie użytkownika o Niepoprawne logowanie użytkownika o Niepoprawne logowanie użytkownika w przypadku nieprawidłowego podania hasła o Aktywność logowania ze wskazaniem adresu IP użytkownika/stacji roboczej • System musi umożliwiać audyt zmian na kontach użytkowników Azure Active directory, a w szczególności: o Ostatnio utworzony użytkownik o Ostatnio usunięty użytkownik o Ostatnio zaktualizowany użytkownik o Ostatnio aktywowany użytkownik o Ostatnio dezaktywowany użytkownik o Ostatnio zmienione hasło dla użytkownika o Ostatnio zresetowane hasło dla użytkownika • System musi umożliwiać Audyt nadanych ról w Azure Active Directory, a w szczególności: o Ostatnio przypisany członek do roli o Ostatnio odłączony członek od roli • System musi umożliwiać audyt zmian grup w Azure Active Directory, a w szczególności: o Ostatnio utworzona grupa o Ostatnio usunięta grupa o Ostatnio zaktualizowana grupa o Ostatnio dodani członkowie do grup o Ostatnio usunięci członkowie z grup • System musi umożliwiać audyt urządzeń USB dla Serwerów Windows 2016 i systemu Windows 10, a w			

	szczególności: ○ Zmiany na plikach lub folderach ○ Odczyt danego pliku ○ Zmiana danego pliku ○ Kopiowane danego pliku • System musi umożliwiać analitykę zachowań, pokazując dane sumarycznie, a w szczególności: ○ Nietypową aktywność danego użytkownika ○ Nietypową aktywność użytkownika na serwerze ○ Nietypową ilość prób np. logowań ○ Nietypowe godziny logowań użytkowników ○ Nietypowe przydzielenie zasobów (quota) dla danego użytkownika ○ Nietypowe działania na plikach			

2. **Oświadczamy, iż przedmiot niniejszego zamówienia zrealizujemy w terminie do ……..... od daty zawarcia umowy.** *(Zamawiający wymaga, aby termin realizacji zamówienia był nie dłuższy niż do 21 dni od daty zawarcia Umowy).*
3. **Akceptujemy warunki płatności podane w Ogłoszeniu o zamiarze udzielenia zamówienia.**
4. **Osobą upoważnioną do kontaktów z Zamawiającym, w celu realizacji umowy jest: p**……..……., tel./faks:……..……., e-mail:……..
5. **Zastrzegamy sobie prawo zmiany ww. osoby**, w drodze pisemnej notyfikacji o dokonanej zmianie.
6. **Wraz z niniejszą ofertą składamy:**

Nazwa załącznika	nr strony
1.....	.....
2.....	.....

.....

data i podpis osoby uprawnionej
do reprezentowania Wykonawcy