Załącznik nr 1 do SWZ

System zarządzania i monitorowania systemów IT Politechniki Lubelskiej

Przedmiotem zamówienia jest dostawa niezbędnych licencji systemu zarządzania i monitorowania systemów informatycznych Politechniki Lubelskiej wraz z usługą wdrożenia.

Systemy informatyczne Politechniki Lubelskiej objęte postępowaniem:
1. Domena Active Directory składająca się z 3 kontrolerów domeny. Do domeny obecnie podłączonych jest 30 serwerów Windows Server 2019 i 2022, w tym dwa serwery plików.
2. System poczty elektronicznej oparty o rozwiązanie Microsoft Exchange 2019 (4 serwery typu Mailbox i 2 serwery typu Edge) obsługującego 1600 skrzynek pocztowych.
3. Domena AD Azure.

Systemami zajmuje się 4 administratorów Zamawiającego.

Zakres przedmiotu zamówienia:
- dostawa systemu zarządzania i monitorowania systemów informatycznych Politechniki Lubelskiej,
- instalacja rozwiązania w infrastrukturze wirtualizacji serwerów ESXi Zamawiającego,
- kompleksowa konfiguracja rozwiązania ze funkcjonalnościami dostępnymi w ramach oferowanych licencji,
- przygotowanie dokumentacji powykonawczej,
- przeszkolenie czterech administratorów z obsługi dostarczonego rozwiązania.

Opis funkcjonalny.

I. Moduł raportowania i audytowania domeny ACTIVE DIRECTORY:

Podstawowe funkcjonalności modułu:
1. Moduł musi działać bezagentowo.
2. Moduł musi działać na systemach z rodziny Windows.
3. Moduł powinien umożliwiać na podłączenie certyfikatu, w formacie .PFX oraz Java Keystore.
4. Moduł musi działać w formie aplikacji Internetowej.
5. Moduł obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych.
6. Moduł działa na pojedynczej bazie danych.
7. Moduł umożliwia dzięki wbudowanym mechanizmom/skryptom:
    - backup bazy danych,
    - odtworzenie bazy danych,
    - zmianę bazy danych.
8. Moduł musi używać jednego konta do połączenia z domeną ACTIVE DIRECTORY.
9. Moduł musi posiadać wbudowane oprogramowanie, z interfejsem graficznym, które pozwala na aktualizację aplikacji.
10. Moduł umożliwia zmianę portu HTTP/HTTPS z poziomu interfejsu graficznego.

Funkcjonalności aplikacji:
1. Moduł posiada możliwość aktywacji podwójnej autentykacji techników oprogramowania.

2. Moduł umożliwia audyt zdarzeń zarówno w czasie rzeczywistym jak i w ustawianych interwałach czasowych.
3. Moduł posiada możliwość raportowania wszystkich domen z pomocą pojedynczego raportu.
4. Moduł umożliwia zbiorcze audytowanie środowiska Active Directory oraz posiada wbudowane raporty dotyczące:
    a. Nieudanych próby zalogowania do środowiska domenowego;
    b. Stacji roboczych;
    c. Serwerów;
    d. Kontrolerów domen;
    e. Poprawne logowanie użytkowników wraz z pełną historią logowania;
    f. Nieudane próby logowania na serwery Radius oraz historię logowań;
    g. Zmiany dokonywane na kontach użytkowników, a w szczególności:
        - Tworzenie kont,
        - Usuwanie kont,
        - Dezaktywacja kont,
        - Modyfikacja haseł,
        - Spis zablokowanych użytkowników,
        - Historie użytkowników.
    h. Audyt zmian w grupie obiektów, w grupie bezpieczeństwa, operacje związane z tworzeniem i usuwaniem grup.
    i. Raportowanie użytkowników zagnieżdżonych w innych grupach.
    j. Raport aktywności użytkowników oraz dezaktywacji stacji roboczych przez wylogowanie lub wygaszacz ekranu.
    k. Zmiany dokonane na obiektach komputerów, a w szczególności:
        - Tworzenie kont,
        - Usuwanie kont,
        - Dezaktywację kont,
        - Historię kont.
    l. Audyt zmian w OU, a w szczególności:
        - Tworzenie OU,
        - Usuwanie OU,
        - Listę modyfikowanych OU,
        - Historię OU.
    m. Audyt zmian w zasadach grupowych, a w szczególności:
        - Tworzenie GPO,
        - Usuwanie GPO,
        - Listę zmodyfikowanych GPO,
        - Historia GPO.
    n. Zaawansowane raporty GPO mogą zostać przesłane do systemu SIEM.
    o. 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.
    p. Zmiany w serwerach DNS.
    q. Śledzenie zmian nazw użytkowników/komputerów/grup.

5. Moduł pozwala na zbiorcze audytowanie zmian na serwerach plików, a w szczególności:
    a. Windows,
    b. Windows File Cluster.
6. Moduł posiada możliwość budowania własnych raportów w oparciu o funkcjonalności modułu wraz z możliwością harmonogramowania.
7. Moduł obsługuje regex dla wzorców wykluczania plików.
8. Moduł potrafi audytować wydruki, w tym:
    a. Kto wykonywał wydruk,
    b. Jaki plik drukował,
    c. Kiedy wykonał wydruk,
    d. Ile kopii wykonał,
    e. Jaki był rozmiar pliku,
    f. Ile stron pliku zostało wydrukowane,
    g. Użytą drukarkę,
    h. Na którym serwerze znajduje się drukarka.
9. Moduł pozwala na tworzenie raportów zgodności, a w szczególności posiada wbudowane raporty zgodności dla audytów, a w szczególności: SOX, HIPAA, PCI-DSS, FISMA, RODO/GDPR.
10. Moduł pozwala na audyt:
    a. Zmian na serwerach członkowskich
    b. Audyt stacji roboczych
11. Moduł posiada moduł powiadomień w formie alertów:
    a. Widocznych w systemie
    b. Drogą mailową
    c. Poprzez SMS
12. Moduł umożliwia podczas tworzenia profili alertów e-mail i SMS, listy mailingowej na podstawie wielu zmiennych (np., Nazwa użytkownika, SID itp.)
13. Moduł umożliwia wykonanie różnego rodzaju skryptów, dzięki którym zagrożenie zostaje wyeliminowane natychmiast.
14. Moduł posiada alerty o przekroczonej przestrzeni dyskowej
15. Moduł posiada narzędzie umożliwiające zwolnienie zajętej przestrzeni dyskowej
16. Moduł przechowuje zarchiwizowany zbiór logów z audytowanego środowiska i ma możliwość dokładnego ustawiania czasu przeniesienia do archiwum.
17. Moduł pozwala na audyt Azure Active Directory, a w szczególności:
    a. Poprawne logowanie użytkownika
    b. Niepoprawne logowanie użytkownika
    c. Niepoprawne logowanie użytkownika bazowanego po nieprawidłowym podaniu hasła
    d. Aktywność logowania ze wskazaniem adresu IP użytkownika/stacji roboczej
18. Moduł pozwala na audyt zmian na kontach użytkowników Azure Active Directory, a w szczególności posiada wbudowane raporty dotyczące:
    a. Ostatnio utworzony użytkownik
    b. Ostatnio usunięty użytkownik
    c. Ostatnio zaktualizowany użytkownik
    d. Ostatnio aktywowany użytkownik
    e. Ostatnio dezaktywowany użytkownik
    f. Ostatnio zmienione hasło dla użytkownika
    g. Ostatnio zresetowane hasło dla użytkowników.
19. Moduł pozwala na Audyt nadanych ról w Azure Active Directory, a w szczególności przygotowane raporty dotyczące:
    a. Ostatnio przypisany członek do roli
    b. Ostatnio odłączony członek od roli

20. Moduł pozwala na audyt zmian grup w Azure Active Directory, a w szczególności:
    a. Ostatnio utworzona grupa
    b. Ostatnio usunięta grupa
    c. Ostatnio zaktualizowana grupa
    d. Ostatnio dodani członkowie do grup
    e. Ostatnio usunięci członkowie z grup
21. Moduł umożliwia audyt plików na serwerach, w tym posiada wbudowane raporty dotyczące:
    a. Wszystkich zmian plików i folderów
    b. Plikach zmodyfikowanych
    c. Plikach usuniętych
    d. Plikach przeniesionych
    e. Plikach utworzonych
22. Moduł umożliwia audyt urządzeń USB dla systemów Windows Server 2016/2019 i systemu Windows 10, a w szczególności posiada wbudowane raporty dotyczące:
    a. Zmiany na plikach lub folderach
    b. Odczyt danego pliku
    c. Zmiana danego pliku
    d. Kopiowane danego pliku
23. Moduł umożliwia analitykę zachowań przy użyciu uczenia maszynowego oraz analizy statystycznej, pokazując dane sumarycznie, a w szczególności:
    a. Nietypową aktywność danego użytkownika
    b. Nietypową aktywność użytkownika na serwerze
    c. Nietypową ilość prób np. logowań
    d. Nietypowe godziny logowań użytkowników
    e. Nietypowe działania na plikach
24. Moduł posiada możliwość oceny ryzyka, opartego o uczenie maszynowe:
    a. Użytkownicy połączeni z dużą ilością zasobów
    b. Konta o dużej aktywności
    c. Konta o nadmiernej aktywności
    d. Konta z wysokim % niepowodzeń logowania
    e. Ostatnia aktywność użytkownika
    f. Uśpione konta administratorów
    g. Uprawnienia wykorzystane przez użytkowników
    h. Pierwsze użycie przydzielonego uprawnienia
    i. Konta oparte na zdalnym logowaniu
25. Moduł obsługuje audytowanie zmian na zasobach sieciowych, w tym posiada przygotowane raporty dotyczące:
    a. Zmiany nazw plików oraz folderów
    b. Utworzenie nowych plików oraz folderów
    c. Usunięcie plików oraz folderów
    d. Przeniesienie plików oraz folderów
    e. Zmiany uprawnień na plikach i folderach
26. Moduł umożliwia przesyłanie logów do systemu SYSLOG lub innych systemów SIEM.
27. Moduł obsługuje połączenie LDAP z wykorzystaniem protokołu SSL.
28. Moduł pozwala na eksportowanie raportów/danych do formatów: CSV, PDF, XLS, HTML.
29. Moduł dostarcza informacje o bezpiecznych powiązaniach LDAP, niezabezpieczonych powiązaniach oraz powiązaniach, które zostały odrzucone z powodu błędów.
30. Moduł dodatkowo obsługuje raportowanie z ADLDS oraz LAPS.
31. Moduł potrafi przetworzyć dane do systemu SIEM, w formacie RFC 3164 lub RFC 5424, w tym obsługuje wysyłanie danych po UDP jak i TCP.

32. Moduł potrafi archiwizować dane do plików .zip oraz dołączać je do bazy danych, na żądanie administratora, w tym system pozwala na archiwizację wybranej kategorii zdarzeń.
33. Moduł potrafi zaimportować pliki .evt oraz .evtx, przetworzyć je wg. własnych filtrów oraz prezentować, jak resztę danych.
34. Moduł pozwala na określenie godzin biznesowych, w celu filtrowania prezentowania raportów, na podstawie godzin pracy, jak i godzin poza pracą.
35. Moduł pozwala na uruchomienie dowolnego programu, w momencie wystąpienia alertu.
36. Moduł obsługuje wiele domen na pojedynczej instancji.
37. Moduł pozwala na pobieranie danych z AzureAD, w tym przetworzenia ich wg. własnych wbudowanych reguł.
38. Moduł posiada możliwość wyszukiwania własnych, wbudowanych raportów, na podstawie słów kluczowych.
39. Moduł posiada możliwość śledzenia wiersza poleceń użytych przez proces.
40. Moduł umożliwia konfigurację wysokiej wydajności.

II. Moduł zarządzania domeną ACTIVE DIRECTORY

Podstawowe funkcjonalności modułu:

1. Moduł posiada wbudowany moduł, pozwalający na skonfigurowanie failover, na podstawie drugiej instancji.
2. Moduł działa w formie aplikacji Internetowej.
3. Moduł umożliwia na podłączenie certyfikatu, w formacie .PFX(PKCS12) oraz Java Keystore.
4. Moduł działa na pojedynczej bazie danych.
5. Moduł działa na systemach z rodziny Windows.
6. Moduł posiada wbudowane skrypty, które pozwalają na:
    a. backup bazy danych,
    b. odtworzenie bazy danych,
    c. zmianę bazy danych.
7. Moduł obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania własnych danych.
8. Moduł umożliwia podłączenie własnego skryptu, przy tworzeniu nowego użytkownika.
9. Moduł posiada specjalnie przygotowane API, które pozwala na utworzenie nowego użytkownika w wybranej domenie.
10. Moduł używa jednego konta do połączenia z domeną.
11. Moduł posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
12. Moduł potrafi na zmianę portu HTTP/HTTPS z poziomu interfejsu graficznego.
13. Moduł posiada wbudowany moduł workflow, który pozwala na akceptację danej akcji, zażądanej przez zgłaszającego, w tym:
    a. Moduł workflow posiada 3 etapy akceptacji:
        - Przegląd - weryfikacja danych
        - Akceptacja
        - Wykonanie
    b. Moduł workflow posiada możliwość wymuszenia akceptacji oraz przeglądu, przez określoną ilość osób, gdzie maksymalna ilość osób to 5.

Funkcjonalności aplikacji:

1. Moduł umożliwia zbiorcze zarządzanie użytkownikami Active Directory, a w szczególności:
    a. Tworzenie i modyfikację grup Active Directory

b. Tworzenie kont użytkowników dla wielu użytkowników, w tym unikanie tworzenia duplikatów, poprzez wykorzystywanie dodatkowych elementów w loginie.
c. Modyfikacja atrybutów dla wielu użytkowników
d. Reset haseł i odblokowanie kont dla wielu kont użytkowników
e. Zmianę wyświetlanej nazwy użytkownika
f. Tworzenie skrzynek mailowych systemu Exchange
g. Udostępnianie / blokowanie / usuwanie nieaktywnych kont w Active Directory
h. Przenoszenie użytkowników między jednostkami organizacyjnymi (OU)

2. Moduł umożliwia zbiorcze tworzenie nowych użytkowników w Active Directory, a w szczególności:
   a. Tworzenie użytkowników przez definiowanie wszystkich atrybutów z uwzględnieniem usług Exchange, Terminal, Lync, Office365
   b. Dodawanie użytkowników przez kopiowanie właściwości innego użytkownika.
   c. Import właściwości użytkownika z plików CSV, gdzie jedynym obowiązkowym atrybutem jest nazwa użytkownika.
   d. Tworzenie i wykorzystanie szablonów z wspólnymi atrybutami.
   e. Tworzenie użytkowników w istniejącym kontenerze lub tworzenie nowej jednostki organizacyjnej (OU) i dodanie do niej użytkowników.
3. Moduł posiada możliwość wyświetlenia specyfikacji grup stworzonych za pomocą pliku CSV
4. Moduł umożliwia zbiorcze modyfikowanie kont użytkowników w Active Directory, a w szczególności:
   a. Dla atrybutów ogólnych:
      i. Reset haseł, a w szczególności:
         - Reset haseł dla wielu kont
         - Ustawianie haseł nigdy nie wygasających
         - Ustawianie haseł, których użytkownik nie może zmienić
         - Ustawianie haseł, które użytkownik ma obowiązek zmienić przy następnym logowaniu
         - Usuwanie i blokowanie użytkowników, jeżeli ich hasło wygasło
      ii. Modyfikację formatów nazwy, nazwy wyświetlanej, nazwy logowania I nazwy kont SAM (Security Account Manager).
      iii. Udostępnianie / blokowanie użytkowników, odblokowywanie użytkowników, definiowanie czasu wygaśnięcia kont.
      iv. Definiowanie katalogów głównych (Home Folder), profile i ścieżek skryptów dla użytkowników.
      v. Aktualizację członkostwa grup i list dystrybucyjnych.
      vi. Przenoszenie użytkowników do innych kontenerów.
   b. Dla kont Exchange:
      i. Tworzenie skrzynek na serwerze Exchange dla użytkowników.
      ii. Definiowanie wielkości wiadomości przychodzących i wychodzących oraz innych ograniczeń.
      iii. Ograniczenie limitów adresatów i adresów przekierowania dla użytkowników.
      iv. Modyfikację limitów składowania poczty i retencji usuniętych obiektów.
      v. Udostępnianie/blokowanie dostępu mobilnego do programu Outlook (również w wersji Web), protokołów IMAP4 i POP3.
   c. Dla kont usług terminalowych:
      i. Modyfikację katalogu głównego usług terminalowych i ścieżek profilowych dla użytkowników.

ii. Modyfikację programów startowych dla użytkowników logujących się z usług terminalowych.
iii. Modyfikację czasu trwania sesji, limitu aktywnych sesji, limitu bezczynnych sesji, itd.
iv. Udostępnianie/blokowanie parametrów zdalnej kontroli.

5. Moduł umożliwia zarządzanie kontami użytkowników nieaktywnych i zablokowanych, a w szczególności:
   a. Wyszukiwanie kont użytkowników lub stacji roboczych nie logowanych przez zdefiniowaną ilość dni
   b. Wyszukiwanie wygasłych i niewykorzystywanych kont Active Directory
   c. Lokalizację nieaktywnych kont użytkowników lub stacji roboczych i blokowanie, usuwanie, przenoszenie lub aktywację tych kont.
   d. Prezentację zablokowanych kont, czas ostatniego logowania / wylogowania, rodzaj systemu operacyjnego, itd.
   e. Eksport raportów do plików CSV,XLS, XLSX,HTML,PDF i CSVDE
6. Moduł umożliwia zarządzanie stacjami roboczymi w Active Directory, a w szczególności:
   a. Zbiorcze dodawanie / usuwanie stacji roboczych z grup
   b. Zbiorcze przypisanie ogólnych atrybutów takich jak opis, lokalizacja, itp. do stacji roboczych
   c. Zbiorcze blokowanie / odblokowanie stacji roboczych
   d. Zbiorcze przenoszenie stacji roboczych pomiędzy jednostkami organizacyjnymi (OU) w domenie
7. Moduł umożliwia zarządzanie udziałami plików na serwerach plików, a w szczególności:
   a. Zbiorcze modyfikowanie uprawnień NTFS do plików/folderów
   b. Zbiorcze usuwanie uprawnień NTFS do plików/folderów
   c. System posiada możliwość raportowania dostępu do poszczególnych folderów
8. Moduł posiada gotowy zestaw wbudowanych raportów:
   a. Raport użytkowników
   b. Raport bezpieczeństwa
   c. Raport logowania
   d. Raport z usługi Exchange
   e. Raport haseł
   f. Raport GPO
   g. Raport stacji roboczych
   h. Raport grup
   i. Raport polis
   j. Raport jednostek organizacyjnych
   k. Raport udziałów NTFS
   l. Raport uprawnień i dostępu do katalogów
9. Moduł posiada możliwość zarządzania i raportowania Office365:
   a. Możliwości raportowania:
      i. Raporty użytkowników
      ii. Raporty grup
      iii. Raporty kontaktów
      iv. Raporty licencji
      v. Raporty skrzynek pocztowych
      vi. Raporty OWA
   b. Możliwości zarządzania:
      i. Zarządzenie użytkownikami
      ii. Zarządzenia grupami
      iii. Zarządzanie kontaktami
      iv. Zarządzanie licencjami

v. Zarządzanie skrzynkami mailowymi
vi. Zarządzanie udostępnionymi skrzynkami mailowymi
vii. Zarządzanie kalendarzem

10. Moduł potrafi udostępniać różne poziomy dostępu tak, aby możliwa była delegację zadań do pracowników działu wsparcia IT i innych działów bez konieczności dystrybucji uprawnień administratora, z możliwością ograniczenia zadań do poszczególnych jednostek organizacyjnych oraz domen, a w szczególności:
    a. Reset hasła użytkownika
    b. Odblokowanie konta użytkownika
    c. Dodawanie i usuwanie członków grup
    d. Przenoszenie użytkowników do różnych jednostek organizacyjnych w ramach domeny
    e. Dodawanie i usuwanie stacji roboczych w domenie
    f. Tworzenie kont użytkowników
    g. Tworzenie, usuwanie i modyfikacja atrybutów kont użytkowników
11. Moduł umożliwia definiowanie procedur przebiegu pracy (pętli warunkowych) z możliwością tworzenie przynajmniej czterech typów wykonawców procedur: zgłaszający, recenzent, zatwierdzający i wykonawca.
12. Moduł udostępnia API, przez które można:
    a. Tworzyć OU
    b. Tworzyć użytkownika, wg. Predefiniowanych w systemie szablonów
    c. Restartować hasło użytkownika
    d. Odblokować/zablokować użytkownika
    e. Usunąć użytkownika
    f. Wyszukać konkretnego użytkownika w AD, wraz z możliwością:
        i. Wyszukania go przy pomocy tekstu
        ii. Wymuszenia synchronizacji z AD, przed podaniem wyników wyszukiwania
        iii. Posortowania wyników według wybranej kolumny
        iv. Posortowania wyników rosnąco lub malejąco
    g. Ustawić datę, w której wygaśnie konto użytkownika.
13. Moduł potrafi przedstawiać podstawowe dane dotyczące Active Directory na pulpicie Administratora, w tym:
    a. Wyświetlać ilość wszystkich użytkowników
    b. Wyświetlać ilość nieaktywnych użytkowników, w ciągu 30 dni
    c. Wyświetlać ilość zablokowanych użytkowników
    d. Wyświetlać ilość wyłączonych użytkowników
    e. Wyświetlać ilość użytkowników z wygaśniętym hasłem
    f. Wyświetlać ilość użytkowników, którzy nigdy się nie zalogowali
    g. Wyświetlać ilość użytkowników, którzy zalogowali się w ciągu ostatnich 30 dni
    h. Wyświetlać ilość komputerów wszystkich
    i. Wyświetlać ilość nieaktywnych komputerów, w ciągu 30 dni.
    j. Mieć możliwość reprezentacji danych dla różnych domen
    k. Wyświetlać szczegółowe dane, po przejściu do widżetu
14. Moduł pozwala na wysyłanie notyfikacji e-mailowych odnośnie wykonywanych akcji w systemie.
15. Moduł umożliwia modyfikację polityk GPO wraz z ustawianiem poszczególnych parametrów.
16. Moduł pozwala na włączenia mechanizmu captcha podczas logowania użytkowników systemu.
17. Moduł potrafi wykonać kopię zapasową obiektów z Active Directory.
18. Moduł umożliwia na dodawanie własnych atrybutów LDAP z AD do raportów.
19. Moduł posiada możliwość przeszukiwania AD oraz przesyłanie wyniku do pliku.

20. Moduł posiada możliwość tworzenia cyklicznych raportów oraz przesłanie wyników drogą mailową.
21. Moduł pozwala na konfigurację automatyzacji w oparciu o własny raport.
22. Moduł posiada możliwość powiadamiania administratorów, jeśli moduł zostanie wyłączony.
23. Moduł posiada możliwość tworzenia/usuwania użytkowników lub grup jak i tworzenia zapytania do workflow z pomocą REST API.
24. Moduł posiada możliwość wykonania skryptu z wybranej ścieżki lub z innej bazy danych jak Oracle oraz MSSQL.
25. Moduł posiada możliwość zarządzania kanałami i politykami w Microsoft Teams.
26. Moduł ma możliwość automatycznego wykonywania krytycznych zadań, jak i zamykanie aktywnych sesji w Office365.
27. Dla modułu „Backup" system posiada funkcję „ElasticSearch" w celu uproszczenia przeszukiwania kopii zapasowych.

III. Moduł monitorowania i audytu systemu poczty elektronicznej (MS Exchange 2019)

Podstawowe funkcjonalności modułu:

1. Moduł posiada możliwość działania na systemie bazodanowym MSSQL, również na klastrze MSSQL.
2. Moduł działa na systemach z rodziny Windows.
3. Moduł działa na podłączenie certyfikatu, w formacie .PFX(PKCS12) oraz Java Keystore.
4. Moduł analizuje dane pochodzące z logów serwerów Exchange.
5. Moduł analizuje dane, które samodzielnie pobiera z serwerów IIS.
6. Moduł działa bezagentowo.
7. Moduł potrafi przechowywać zarchiwizowany zbiór logów z audytowanego środowiska i mieć możliwość dokładnego ustawiania czasu przeniesienia do archiwum.
8. Moduł potrafi przypominać użytkownikom o wygaśnięciu hasła.
9. Moduł obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych.
10. Moduł posiada wbudowane skrypty, które pozwalają na:
    a. backup bazy danych,
    b. odtworzenie bazy danych,
    c. zmianę bazy danych.
11. Moduł używa jednego konta do połączenia z domeną.
12. Moduł posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
13. Moduł pozwala na zmianę portu HTTP/HTTPS z poziomu interfejsu graficznego.

Funkcjonalności aplikacji:

1. Moduł obsługuje serwery Microsoft Exchange w wersjach: 2016, 2019.
2. Moduł posiada wbudowany dashboard, pokazujący najważniejsze dane z całego środowiska Exchange oraz dodatkowy dashboard dla Exchange Online, w którym prezentuje:
    a. Wszystkie serwery Exchange, wraz z:
        i. Statusem ich usług,
        ii. Zużyciem ich dysku,
        iii. Statusu przepływu poczty,
        iv. Statusu kolejki pocztowych,
    b. Raporty graficzne, dotyczące:
        i. Użycia dysku, w rozbiciu na:
            - Wolne miejsce,

- Miejsce zajęte przez bazy danych,
- Miejsce zajęte przez inne pliki,

ii. Największych skrzynek pocztowych,
iii. Ilości wysłanych e-mail'i
iv. Ilości odebranych e-maili,
v. Wielkości odebranych e-maili,
vi. Wielkości wysłanych e-maili,
vii. Wysłanych e-mail'i per serwer Exchange,
viii. Odebranych e-maili per serwer Exchange,
ix. Ilości skrzynek z włączoną opcją prześlij dalej,
x. Typu skrzynek, z podziałem na:
    - Skrzynki użytkownika,
    - Skrzynki pokojów,
    - Skrzynki publicznych folderów,
    - Skrzynki udostępnione,
    - Skrzynki przedmiotów,
xi. Ilości skrzynek na każdy serwer.
xii. Raport aktywności skrzynek pocztowych (Mailbox Traffic Report) - Liczba wiadomości według nadawcy na podstawie statusu odbiorcy.
xiii. Raport aktywności list dystrybucyjnych (Disctribution Lists Traffic Reports):
    - Liczba wiadomości wysłanych przez grupy dystrybucyjne.
    - Rozmiar wiadomości wysyłanych przez grupy dystrybucyjne.
    - Liczba wiadomości wysłanych przez grupy dystrybucyjne na podstawie statusu odbiorcy.
    - Liczba wiadomości otrzymanych przez grupę dystrybucyjną.
    - Rozmiar wiadomości otrzymywanych przez grupę dystrybucyjną.
    - Ruch przesyłowy dla grup dystrybucyjnych.
    - Odebrany ruch dla grup dystrybucyjnych.
    - Liczba wysłanych i odebranych wiadomości.
xiv. Raport aktywności per jednostka Organizacyjna (Organizational Unit Traffic Reports)
    - Liczba wiadomości wysłanych przez jednostkę organizacyjną.
    - Rozmiar wiadomości wysyłanych przez jednostkę organizacyjną.
    - Liczba wiadomości wysłanych przez jednostkę organizacyjną na podstawie statusu odbiorcy.
    - Liczba wiadomości otrzymanych przez jednostkę organizacyjną.
    - Rozmiar wiadomości otrzymywanych przez jednostkę organizacyjną.
    - Liczba wysłanych i odebranych wiadomości.
xv. Raport aktywności grup (Group Traffic Reports)
    - Liczba wiadomości wysłanych przez grupy.
    - Rozmiar wiadomości wysyłanych przez grupy.
    - Liczba wiadomości wysłanych przez grupy na podstawie statusu odbiorcy.
    - Liczba wiadomości otrzymanych przez grupę.
    - Rozmiar wiadomości otrzymywanych przez grupę.
    - Liczba wysłanych i odebranych wiadomości.
xvi. System posiada raporty dostępów do Exchange Online dla:
    - Skrzynek pocztowych
    - Udostępnionych skrzynek pocztowych
    - Publicznych folderów

- Kalendarza

3. Moduł posiada dashboard dla serwerów Skype, w którym prezentuje raporty graficzne, dotyczące:
   a. Użytkowników, którzy wykonali największą ilość połączeń,
   b. Użytkowników, którzy przesłali najwięcej plików wewnątrz organizacji,
   c. Użytkowników, którzy przesłali najwięcej plików poza organizację.
4. Moduł umożliwia użytkownikom możliwość analizy, raportowania i audytu serwerów Microsoft Exchange, a w szczególności posiada wbudowane raporty dotyczące:
   a. Raportowanie przychodzących i wychodzących wiadomości e-mail
   b. Raportowanie wielkości skrzynek pocztowych
   c. Raportowanie ruchu w skrzynkach pocztowych
   d. Raportowanie zawartości skrzynek pocztowych
   e. Monitorowanie liczby wiadomości wysłanych i odbieranych przez każdy serwer programu Exchange, używając raportów o ruchu na serwerze.
   f. Monitorowanie istotnych statystyk folderów publicznych serwera programu Exchange, za pomocą raportów o folderze publicznym
   g. Raportowanie list dystrybucyjnych i ruchu na każdej z list
   h. Raportowanie uprawnień do skrzynek pocztowych
   i. Raportowanie uprawnień do folderów publicznych wraz z podfolderami.
   j. Raportowanie usługi OWA (Outlook Web Access)
   k. Audyt logowania do skrzynek pocztowych
   l. Audyt zmian uprawnień na skrzynkach pocztowych
   m. Audyt zmian ustawień na skrzynkach pocztowych
   n. Audyt zmian uprawnień na folderach publicznych.
   o. Audyt zmian bazy danych
   p. Raport zmian w grupach dystrybucyjnych
   q. Raport zmian w członkostwie grup dystrybucyjnych
5. Moduł umożliwia monitoring i raportowanie aktywności serwerów Exchange w wersji 2019, a w szczególności komponentów:
   a. **Serwer Exchange**, a w szczególności:
      i. Raportowanie statusów stanu zdrowia usług Exchange
      ii. Raportowanie statusów stanu zdrowia usług replikacji skrzynek pocztowych (MRS)
      iii. Raportowanie statusów stanu zdrowia przepływu poczty email
      iv. Raportowanie statusów stanu wykorzystania CPU
      v. Raportowanie statusów stanu wykorzystania pamięci RAM
      vi. Raportowanie statusów stanu połączeń serwerów Exchange z innymi komponentami i protokołami, a w szczególności:
         - Połączeń z ActiveSync
         - Połączeń z OWA (Outlook Web Access)
         - Połączeń z Internet Message Access Protocol
         - Połączeń z Post Office Protocol
         - Połączeń z usługami Web
         - Połączeń z Exchange Control Panel
   b. **DAG** (Database Availability Group), a w szczególności:
      i. Raportowanie statusów stanu zdrowia usług replikacji
      ii. Raportowanie statusów stanu wykonania kopii zapasowej bazy danych
   c. **Baza danych Exchange**, a w szczególności:
      i. Raportowanie statusów stanu zdrowia funkcji ExchangeSearch
      ii. Raportowanie statusów połączeń z MAPI
      iii. Raportowanie statusów stanu wykonania backupów bazy danych

6. Moduł umożliwia monitorowanie i raportowanie z Exchange Online, w tym:
    a. Raportowanie o:
        i. Ilości użytkowników,
        ii. Nieaktywnych skrzynkach,
        iii. Użytkownikach, z uprawnieniami Wyślij jako/wyślij w imieniu,
        iv. Niedawno utworzonych skrzynkach
        v. Odłączonych skrzynkach
        vi. Regułach poczty przychodzącej,
        vii. Wyszukiwania wiadomości po tytule wiadomości,
        viii. Niedostarczonych wiadomościach,
        ix. Wiadomościach wysłanych do niewłaściwych adresatów,
        x. Porównania dostarczonych kontra niedostarczonych,
        xi. Ilości logowań do OWA per użytkownik,
        xii. Ilości urządzeń mobilnych,
        xiii. Nieaktywnych/aktywnych urządzeniach mobilnych,
        xiv. Urządzeniach mobilnych, z podziałem na system operacyjny,
        xv. Skrzynkach udostępnionych,
        xvi. Niedawno utworzonych wydarzeniach w kalendarzu,
        xvii. Niedawno zmodyfikowanych wydarzeniach w kalendarzu,
        xviii. Nieaktywnych listach dystrybucji,
        xix. Nieaktywnych urządzeniach ActiveSync
7. Moduł posiada możliwość audytowania zmian w Exchange Online, takich jak:
    a. Akcje wykonane przez administratorów Exchange,
    b. Aktywności typu „wyślij jako”,
    c. Zmiany w kalendarzach,
    d. Utworzenie, usunięcie oraz modyfikacja kontaktu
    e. Zmiany w quota,
    f. Utworzenie, usunięcie oraz modyfikację folderu publicznego,
    g. Aktywność przesunięcia e-mail’a lub usunięcia,
    h. Zmiany ustawień connector’ów
8. Moduł posiada możliwość modyfikacji interwału odpytywania Exchange Online, od minimalnie 5 minut, do 24 godzin oraz posiada możliwość wymuszenia pobrania danych.
9. Moduł umożliwia filtrowanie wszystkich akcji audytowych, na bazie:
    a. Godzin biznesowych,
    b. Kolumn w prezentowanym w raporcie, na wszystkich typach danych, w tym:
    c. Daty,
    d. Nazwy,
    e. Adresy IP
10. Moduł posiada możliwość wykonania raportów zgodności, w standardzie SOX, HIPAA, PCI, GLBA, GDPR.
11. Moduł umożliwia monitoring i raportowanie konfiguracji skrzynek pocztowych, w szczególności:
    a. Skrzynek z włączoną opcją przekazywania poczty na domenę zewnętrzną
    b. Skrzynek z włączoną opcją przekazywania poczty na domenę wewnętrzną
    c. Skrzynek bez włączonej opcji przekazywania poczty
    d. Skrzynek bez ustawionego zdjęcia
    e. Skrzynek, które mają możliwość wykorzystania ActiveSync.
    f. Skrzynek, które posiadają reguły poczty przychodzącej
    g. Skrzynek, które mają konfigurację wiadomości śmieci
12. Moduł umożliwia monitoring i raportowanie:
    a. Tworzenia list dystrybucyjnych
    b. Usuwania list dystrybucyjnych

c. Modyfikację użytkowników listy dystrybucyjnej
d. Skrzynek, które posiadają nieprzeczytane wiadomości e-mail'owe

13. Moduł umożliwia raportowanie użytkowników z:
    a. Uprawnieniami “wyślij jako”
    b. Uprawnieniami “wyślij w imieniu”
14. Moduł umożliwia raportowanie aplikacji Skype for business, w szczególności:
    a. Polityk kodów PIN
    b. Konferencji wszystkich lub per użytkownik
    c. Nieaktywnych użytkowników
    d. Konfiguracji konferencji
    e. Aktywności wiadomości IM
    f. Rozmów Audio/Video
    g. Nieprzypisanych numerów
    h. Polityk głosowych
    i. Przesyłania plików
15. Moduł umożliwia utworzenie własnych niestandardowych raportów, na bazie istniejących raportów w systemie, które mogą zostać zabezpieczone hasłem.
16. Moduł umożliwia na utworzenie zaplanowanych raportów, które będą wysyłane co cykliczny, określony przez użytkownika, okres czasu, w następujących formatach: PDF, CSV, XLS, HTML oraz w następujących, możliwych konfiguracjach cyklicznego wysyłania:
    a. Codziennie,
    b. Raz na tydzień,
    c. Raz na miesiąc.
17. Moduł umożliwia na automatyczne zarządzenie dostępną pulą licencji, w wybranych godzinach, w oparciu o atrybuty skrzynki, takie jak:
    a. Nazwę serwera,
    b. Domenę,
    c. Czy jest ukryta,
    d. Czy jest wyłączona,
    e. Bazę danych,
    f. OU.
18. Moduł dodatkowo zapisuje wszystkie zaplanowane raporty na dysku.
19. Moduł umożliwia audytowanie raportów wyeksportowanych przez użytkowników aplikacji
20. Moduł umożliwia eksportowanie raportów do plików XLS, CSV, PDF, HTML zabezpieczonych opcjonalnym hasłem.
21. Moduł umożliwia dołączyć niestandardowe atrybuty z schematu Active Directory do raportów.
22. Moduł umożliwia wymuszenie złożoności haseł dla nowych administratorów i operatorów.
23. Moduł samodzielnie analizuje dane pochodzące serwerów Exchange, pobranych przy pomocy:
    a. PowerShell,
    b. EventLog serwera Exchange,
    c. Logów serwerów IIS,
24. Moduł pozwala na wybranie niestandardowej ścieżki logów IIS oraz logów ról transportowych.
25. Administratorzy mogą stworzyć i zdefiniować role dla operatorów systemu.
26. Moduł umożliwia filtrowanie danych w oparciu o grupy administracyjne, grupy routingu i inne kryteria.
27. Moduł posiada moduł powiadomień, w formie informacji:
    a. Widocznych w systemie,

   b. Wysyłanych drogą mailową,
28. Moduł powiadomień, pozwala na utworzenie alertów dla wszystkich akcji, na środowisku Exchange i Exchange Online, oraz na filtrowanie ich na bazie:
   a. Parametrów eventu,
   b. Wartości brzegowych ilości wydarzeń,
29. Moduł pozwala na przesyłanie zebranych przez siebie logów, do zewnętrznego systemu SIEM.
30. Moduł posiada możliwość audytu akcji techników.
31. Moduł posiada możliwość tworzenia harmonogramów dla automatycznego zarządzania licencjami.
32. Moduł umożliwia włączenie podwójnej autentykacji techników do oprogramowania.

Zapisy ogólne.

Zamawiający wymaga, aby wszystkie dostarczane pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie realizujące wszystkie wymagane funkcje musiało być dostępne na rynku co najmniej 12 miesięcy przed terminem składania ofert. Oprogramowanie systemowe musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowania np. w wersji Beta) w chwili, i co najmniej w okresie 12 miesięcy przed terminem złożenia ofert. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie producenta rozwiązania.

Zamawiający wymaga, aby zaoferowany system zarządzania i monitoringu systemów IT był dostępny i wspierany przez producenta oraz nie będzie przez niego przewidziany do wycofania ze sprzedaży i wsparcia w najbliższym czasie (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life).

Wdrożenie.

Wykonawca uruchomi oferowany system zarządzenia i monitoringu systemów informatycznych Politechniki Lubelskiej i wykona konfigurację zgodną z funkcjonalnością zamawianego systemu oraz dokona instalacji wszystkich niezbędnych licencji w terminie do 30 dni od daty podpisania umowy. Na potrzeby wykonania przez Wykonawcę konfiguracji zamawianego systemu zarządzenia i monitoringu systemów informatycznych, Wykonawca, przed wdrożeniem, opracuje i przedstawi do akceptacji Zamawiającego koncepcje konfiguracji systemu na podstawie danych przekazanych przez Zamawiającego. Do tego celu Zamawiający przekaże Wykonawcy wszystkie niezbędne informacje potrzebne do konfiguracji systemu. Na potrzebę instalacji i konfiguracji rozwiązania w środowisku wirtualnym Zamawiający przygotuje niezbędne dostępy dla Wykonawcy (dostęp przez VPN, dedykowane konto w VCenter).

Prace wdrożeniowe mają objąć minimum:

1. Konfigurację podstawową systemu (konfiguracja sieciowa, konta administratorów, aktualizacja oprogramowania do najnowszej wersji).
2. Wgranie wszystkich licencji zaoferowanego rozwiązania. Aktywacja (o ile wymagane) dostarczonych licencji na utworzonym w portalu producenta koncie dla Zamawiającego.
3. Instalacja oraz konfiguracja modułów.
4. Konfiguracja komponentów i uruchomienie usług wymaganych zakresem przedmiotu zamówienia.

Wykonawca zapewni do realizacji przedmiotu zamówienia przydzielenie przynajmniej dwóch inżynierów posiadających certyfikat producenta lub dystrybutora oferowanego rozwiązania potwierdzające wiedzę z zakresu wdrażania i administracji oferowanym rozwiązaniem.

Wsparcie techniczne.

Wykonawca zapewni wsparcie techniczne producenta dla dostarczanego systemu będącego przedmiotem zamówienia, obejmującego w pełnym zakresie dostarczone i wdrożone elementy zamówienia, przez okres 12 miesięcy od daty uzyskania potwierdzenia uruchomienia licencji.

W ramach wsparcia zgłoszenia będą realizowane telefonicznie lub za pomocą systemu informatycznego Wykonawcy lub producenta oprogramowania.
Wykonawca zapewni dostęp do producenckiej bazy aktualizacji oprogramowania, w ramach którego zagwarantowane jest:

a. możliwość pobierania aktualizacji całej oferty oprogramowania związanego z rodzajem dostarczanych licencji;
b. możliwość logowania i pobierania oprogramowania ze strony internetowej producenta licencji w dowolnym momencie, przez cały okres trwania oferowanej usługi wsparcia technicznego.

Dostawa Oprogramowania i licencji.

1. Wykonawca dostarczy oprogramowanie wraz z licencjami do korzystania z oprogramowania w ilości niezbędnej do uruchomienia całego przedmiotu zamówienia, w pełnej wymaganej funkcjonalności.
2. Wykonawca dostarczy najnowsze wersje oprogramowania, zgodnie z informacjami publikowanymi przez producenta danego oprogramowania.
3. Dostarczone oprogramowanie/licencje będą posiadały minimum 12-miesięczne wsparcie techniczne producenta oprogramowania.
4. Do Oprogramowania Wykonawca dostarczy komplet dokumentacji (dotyczącej instalacji, konfiguracji i obsługi) w formie papierowej lub elektronicznej w języku polskim lub angielskim.
5. W przypadku zaoferowania rozwiązania opartego o technologie Microsoft którego moduły instalowane będą na maszynach wirtualnych, Zamawiający posiada do dyspozycji licencje na Windows Server 2022 Data Center dla środowiska wirtualnego.

Szkolenia.

Wymagane jest przeprowadzenie autorskiego szkolenia (w formie warsztatów) z zakresu administracji i obsługi dostarczonego systemu. Zamawiający oczekuje przeszkolenia 4 administratorów systemu, czas trwania szkolenia nie mniejszy niż 2 dni szkoleniowe po 8 godzin dziennie. Szkolenie powinno być realizowane w siedzibie Zamawiającego lub w innym miejscu zaproponowanym przez Wykonawcę, a zaakceptowanym przez Zamawiającego. Zamawiający dopuszcza szkolenie on-line w formie zdalnej. Szkolenie powinno obejmować część praktyczną i teoretyczną i odbywać się zgodnie z zaakceptowanym przez Zamawiającego programem. Wykonawca zapewni uczestnikom materiały dydaktyczne (w formie elektronicznej), co najmniej podręcznik administratora w formie elektronicznej).
Celem szkolenia będzie aby administrator:

1) poznał podstawową konfigurację systemu,
2) poznał wszystkie moduły i funkcjonalności uruchomione w dostarczonym rozwiązaniu,
3) rozumiał zasady i sposób działania systemu,
4) samodzielnie oraz szybko uzyskiwał właściwe i potrzebne informacje z systemu,
5) tworzył raporty dotyczące incydentów i zachowania użytkownika, rozumiał ich powiązania z punktu widzenia funkcjonowania systemu oraz był w stanie monitorować system i rozumiał konsekwencje zmian w konfiguracji.

Dokumentacja powykonawcza.

Dokumentacja powykonawcza zawierać musi co najmniej:

- Wykaz oraz opis przeprowadzonych prac wdrożeniowych.
- Schemat wdrożonej architektury obejmujący wszystkie elementy systemu wraz z adresacją IP oraz portami komunikacyjnymi z i do Systemu.
- Konfiguracja wdrożonego Systemu.
- Loginy i hasła (wdrożeniowe) wszystkich użytkowników, jacy zostali utworzeni we wdrażanych systemach.