Łukasiewicz
Instytut Technik Innowacyjnych EMAG

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa oprogramowania oraz części komputerowych"
– nr postępowania FH/ 02/ 11/22

Oferowany przedmiot zamówienia musi spełniać wymagania określone przez Zamawiającego, tj. posiadać parametry i funkcjonalności nie gorsze (co najmniej takie same lub lepsze) od określonych poniżej.

Zamówienie podzielone jest na 12 części. Zamawiający dopuszcza składanie ofert częściowych.

Część nr 1 - OPOGRAMOWANIE DO AUDYTU ŚRODOWISKA AD - Pakiet dla 16 kontrolerów

Opis oprogramowania	**Oprogramowanie do audytu środowiska ActiveDirectory**
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 16 kontrolerów domeny ActiveDirectry; 2. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji.
Cechy oprogramowania	**Kluczowe funkcjonalności:** 1. System działa bezagentowo. 2. System działa na systemach z rodziny Windows. 3. System pozwala na podłączenie certyfikatu, w formacie .PFX oraz Java keystore. 4. System obsługuje integracje ze Splunk'iem i ArcSight'em 5. System działa w formie aplikacji Internetowej. 6. System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych. 7. System działa na pojedynczej bazie danych. 8. System posiada wbudowane skrypty, które pozwalają na: a) backup bazy danych, b) odtworzenie bazy danych, c) zmianę bazy danych. 9. System używa jednego konta do połączenia z domeną. 10. System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji. 11. System pozwala na zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego. 12. System umożliwia audyt plików na serwerach, w określonym odstępie czasowym bezagentowo lub w czasie rzeczywistym przy użyciu agenta, w tym posiada wbudowane raporty dotyczące: a) Wszystkich zmian plików i folderów b) Plikach zmodyfikowanych c) Plikach usuniętych d) Plikach przeniesionych e) Plikach utworzonych

	13. System 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 **Funkcjonalności aplikacji:** 1. System działa bezagentowo. 2. System obsługuje języki: Chiński, Japoński i Angielski. 3. System działa na systemach z rodziny Windows. 4. System pozwala na podłączenie certyfikatu, w formacie .PFX oraz Java keystore. 5. System obsługuje integracje ze Splunk'iem i ArcSight'em 6. System działa w formie aplikacji Internetowej. 7. System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych. 8. System działa na pojedynczej bazie danych. 9. System posiada wbudowane skrypty, które pozwalają na backup bazy danych, odtworzenie bazy danych, zmianę bazy danych. 10. System używa jednego konta do połączenia z domeną. 11. System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji. 12. System posiada możliwość aktywacji podwójnej autentykacji techników oprogramowania. 13. System pozwala na zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego. 14. System umożliwia audyt zdarzeń zarówno w czasie rzeczywistym jak i w ustawianych interwałach czasowych 15. System posiada możliwość raportowania wszystkich domen z pomocą pojedynczego raportu. 16. System 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. 17. Zmiany dokonane na obiektach komputerów, a w szczególności: a) Tworzenie kont b) Usuwanie kont c) Dezaktywację kont d) Historię kont 18. Audyt zmian w OU, a w szczególności a) Tworzenie OU b) Usuwanie OU c) Listę modyfikowanych OU d) Historię OU 19. Zmiany wartości OU oraz domen mogą zostać przesłane do ArcSight. 20. Audyt zmian w zasadach grupowych, a w szczególności: a) Tworzenie GPO b) Usuwanie GPO c) Listę zmodyfikowanych GPO d) Historia GPO 21. Zaawansowane raporty GPO mogą zostać przesłane do systemu SIEM 22. Zaawansowane zmiany w GPO 23. Audyt zmian uprawnień, a w szczególności: a) Uprawnienia dotyczące poziomu dostępu do domeny b) Uprawnienia zmian OU c) Uprawnienia zmian w kontenerach d) Uprawnienia zmian w GPO e) Uprawnienia zmian użytkowników f) Uprawnienia zmian grup g) Uprawnienia zmian komputerów h) Uprawnienia zmian DNS i) Zmiany w DNS'ach j) Śledzenie zmian nazw użytkowników/komputerów/grup 24. System pozwala na zbiorcze audytowanie zmian na serwerach plików, a w szczególności a) Windows b) Windows file Cluster c) EMC d) Net App e) Hitachi NAS 25. System posiada możliwość budowania własnych raportów w oparciu o funkcjonalności systemu wraz z możliwością harmonogramowania 26. System obsługuje regex dla wzorców wykluczania plików. 27. System 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 28. System pozwala na tworzenie raportów zgodności, a w szczególności posiada wbudowane raporty dotyczące: a) Raporty zgodności dla audytów, a w szczególności: b) SOX

	c) HIPAA d) PCI-DSS e) GLBA f) FISMA g) RODO/GDPR 29. System pozwala na audyt: a) Zmian na serwerach członkowskich b) Audyt stacji roboczych 30. System posiada moduł powiadomień w formie alertów a) Widocznych w systemie b) Drogą mailową c) Poprzez SMS 31. System umożliwia podczas tworzenia profili alertów e-mail i SMS, listy mailingowej na podstawie wielu zmiennych (np., Nazwa użytkownika, SID itp.) 32. System umożliwia wykonanie różnego rodzaju skryptów, dzięki którym zagrożenie zostaje wyeliminowane natychmiast. 33. System posiada alerty o przekroczonej przestrzeni dyskowej 34. Narzędzie umożliwia zwolnienie zajętej przestrzeni dyskowej 35. System przechowuje zarchiwizowany zbiór logów z audytowanego środowiska i ma możliwość dokładnego ustawiania czasu przeniesienia do archiwum. 36. System pozwala na audyt Azure Active Directory, a w szczególności: a) Poprawne logowanie użytkownika b) Niepoprawne logowanie użytkownika c) Niepoprawne logowanie użytkownika bazowane na nieprawidłowym podaniu hasła d) Aktywność logowania ze wskazaniem adresu IP użytkownika/stacji roboczej 37. System 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. 38. System 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 39. System 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 40. System umożliwia audyt plików na serwerach, w określonym odstępie czasowym bezagentowo lub w czasie rzeczywistym przy użyciu agenta, w tym posiada wbudowane raporty dotyczące: a) Wszystkich zmian plików i folderów b) Plikach zmodyfikowanych c) Plikach usuniętych

	d) Plikach przeniesionych e) Plikach utworzonych 41. Program posiada możliwość alertowania administratora w razie braku komunikacji z agentem. 42. System umożliwia audyt urządzeń USB dla Serwerów Windows 2016 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 43. System 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 44. System 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 45. System obsługuje audytowanie zmian na share'ach 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 46. System umożliwia przesyłanie logów do SYSLOG'a lub innych systemów SIEM'owych. 47. System obsługuje połączenie LDAP'owe po SSL'u. 48. System pozwala na eksportowanie raportów/danych do formatów: a) CSV b) PDF c) XLS d) HTML 49. System dostarcza informacje o bezpiecznych powiązaniach LDAP, niezabezpieczonych powiązaniach oraz powiązaniach, które zostały odrzucone z powodu błędów. 50. System dodatkowo obsługuje raportowanie z ADLDS oraz LAPS'a. 51. System potrafi przetworzyć dane do systemu SIEM'owego, w formacie RFC 3164 lub RFC 5424, a) W tym obsługuje wysyłanie danych po UDP jak i TCP. 52. System potrafi archiwizować dane do plików .zip oraz dołączać je do bazy danych, na żądanie administratora. a) W tym, system pozwala na archiwizację wybranej kategorii zdarzeń.

	53. System potrafi zaimportować pliki .evt oraz .evtx, przetworzyć je wg. własnych filtrów oraz prezentować, jak resztę danych. 54. System pozwala na określenie godzin biznesowych, w celu filtrowania prezentowania raportów, na podstawie godzin pracy, jak i godzin poza pracą. 55. System pozwala na uruchomienie dowolnego programu, w momencie wystąpienia alertu. 56. System obsługuje wiele domen na pojedynczej instancji. 57. System pozwala na pobieranie danych z AzureAD, w tym przetworzenia ich wg. własnych wbudowanych reguł. 58. System posiada możliwość wyszukiwania własnych, wbudowanych raportów, na podstawie słów kluczowych. 59. System posiada możliwość śledzenia wiersza poleceń użytych przez proces. 60. System umożliwia konfigurację wysokiej wydajności. 61. System posiada raport zmian uprawnień NetApp i EMC w celu dostarczenia informacji o wartościach uprawnień przed i po. 62. System posiada możliwość konfiguracji ustawień agenta. 63. System umożliwia pojedyncze logowanie (SSO) za pośrednictwem NTLM lub SAML. 64. System pozwala na prezentację wszystkich działań użytkowników w jednym raporcie w obszarze Account Management. 65. System umożliwia przeprowadzenie audytu i raportu na temat wykorzystania podatnego na Netlogon połączenie Schannel przez urządzenia z systemem Windows. 66. System pozwala kontrolować dostęp do plików i zmiany uprawnień w systemach pamięci masowej Huawei OceanStor.

Część nr 2 - OPROGRAMOWANIE DO NADZOROWANIA SESJI UPRZYWILEJOWANYCH

Opis oprogramowania	**Oprogramowanie do nadzorowania sesji uprzywilejowanych**
Warunki licencji	1. Licencja nie może ograniczać ilości użytkowników, których w danym momencie sesje są nadzorowane, 2. Licencja powinna umożliwiać nadzorowanie dostęp do co najmniej 25 usług, 3. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji.
Cechy oprogramowania	**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. 2. System musi być zaprojektowany i przygotowany do umieszczenia w DMZ (hardening producenta). 3. System na potrzeby realizacji swoich funkcji nie może wymagać zestawienia tunelu VPN pomiędzy siecią LAN organizacji, a komputerem zewnętrznego dostawcy. Nie może też wykorzystywać technologii chmurowej do nawiązania połączenia.

	4. System musi umożliwiać tryb pracy awaryjnej zapewniający synchronizację danych między dwoma urządzeniami do uprzywilejowanego dostępu zdalnego, tworząc uproszczony proces bezpiecznej wymiany uszkodzonego urządzenia na zapasowe. 5. System musi umożliwiać nawiązywanie sesji przynajmniej w dwóch trybach: a) Z wykorzystaniem instalowanego agenta na systemie, do którego będzie nawiązywana sesja, b) Z wykorzystaniem serwerów proxy bez potrzeby instalacji agenta na systemie, do którego będzie nawiązywana sesja. 6. 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 zewnętrznych dostawców, utworzenie serwera proxy, wyłączenie serwera proxy). 7. Komunikacja między elementami systemu do uprzywilejowanego dostępu zdalnego (tj. oprogramowaniem uprzywilejowanego dostępu zdalnego, agentami instalowanymi na urządzeniach końcowych oraz serwerami proxy) musi być szyfrowana (TLS) i odbywać się na jednym porcie 443. 8. Elementy systemu (agenci, serwery proxy, klienci) instalowani na zasobach i stacjach roboczych muszą umożliwiać pracę w trybie aktywnego nawiązywania połącznia z systemem uprzywilejowanego dostępu zdalnego, tj. bez pozostawiania otwartych portów nasłuchujących na urządzeniach końcowych. 9. System musi posiadać wsparcie dla protokołów SSH, RDP oraz VNC. 10. System musi posiadać możliwość rozbudowy o moduł obsługi sesji do aplikacji WEB (wbudowana przeglądarka WWW). 11. Systemu musi posiadać możliwość uruchomienia sesji aplikacyjnych (uruchomienie wskazanej aplikacji z serwera usług terminalowych lub uruchomienie aplikacji za pomocą dedykowanego agenta) 12. Systemu musi posiadać możliwość tunelowania protokołów TCP na zdefiniowanym porcie między komputerem zewnętrznego dostawcy a zarządzanym systemem. 13. 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. Logowanie dostawców zewnętrznych do systemu uprzywilejowanego dostępu zdalnego musi być zabezpieczone drugim składnikiem (2FA). 3. System musi realizować następujące scenariusze nawiązywania sesji przez zewnętrznego dostawcę: a) za pomocą klienta zainstalowanego na komputerze zewnętrznego dostawcy (gruby klient), b) za pomocą przeglądarki WWW z komputera

	zewnętrznego dostawcy (bez potrzeby instalacji klienta), c) za pomocą klienta zainstalowanego na urządzeniu mobilnym (minimum wsparcie dla systemu Android). 4. System musi umożliwiać opcję zastosowania przez kontraktora własnych klientów RDP i SSH. 5. System musi umożliwiać realizację sesji do stacji roboczych (przynajmniej Windows i Linux) i współdzielenie tej samej sesji między kontraktorem a operatorem pracującym przy stacji roboczej. 6. Rozpoczęcie sesji współdzielonej między kontraktorem a operatorem stacji roboczej musi podlegać procesowi akceptacji przez operatora stacji roboczej do której realizowana jest ta sesja. 7. Rozpoczęcie sesji przez zewnętrznego dostawcę musi podlegać kontroli dostępu poprzez: a) Wysyłanie powiadomień o zdarzeniu rozpoczęcia i zakończenia sesji przez zewnętrznego dostawcę do zdefiniowanej listy osób, b) Ograniczenie możliwości nawiązywania sesji przez zewnętrznych dostawców do określonych dni i godzin, oraz do określonych grup zasobów. c) Włącznie procesu wnioskowania przez zewnętrznego dostawcę o dostęp do zasobów i mechanizmu akceptacji lub odrzucenia wniosku przez właściciela zasobu. We wniosku muszą znaleźć się przynajmniej zakres dat, kiedy zewnętrzny dostawca będzie nawiązywał sesję oraz pole pozwalające opisać zakres wykonywanych przez niego prac. Wniosek musi być wysyłany w celu akceptacji do zdefiniowanej listy osób. 8. Konsola dostępowa dla zewnętrznego dostawcy musi posiadać co najmniej poniższe funkcje: a) widok grup zasobów z możliwością nawiązania sesji do tych zasobów (za pomocą menu kontekstowego lub podwójnego kliknięcia), oraz możliwością wyszukiwania zasobów po ciągach znaków b) szczegółowy opis zasobu, do którego możliwe jest nawiązanie sesji, zawierający nazwę hosta / adres IP, status (aktywny/nieaktywny), typ systemu operacyjnego, edytowalną nazwę skróconą. c) funkcję wieloosobowego chatu działającą między uczestnikami sesji. 9. System musi umożliwić wyłączenie synchronizacji schowka i kopiowania plików między komputerem zewnętrznego dostawcy a zarządzanym zasobem. 10. System w trakcie sesji realizowanej przez zewnętrznego dostawcę musi umożliwiać: a) Dołączenie do sesji dodatkowych użytkowników posiadających konta w systemie uprzywilejowanego dostępu zdalnego; b) 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 braku połączenie autoryzowanego użytkownika ulegnie awarii); c) Przejęcie sesji zewnętrznego dostawcy 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 (zewnętrznego dostawcy), nazwy / adresu IP zarządzanego zasobu, grupy zarządzanych zasobów. 7. System musi posiadać możliwość uruchomienia filtrowania odbytych sesji po ciągach znaków pisanych z klawiatury w trakcie ich trwania. 8. W szczegółach raportu sesji muszą znajdować się co najmniej informacje na temat: a) daty rozpoczęcia i zakończenia sesji (długość trwania sesji), b) nazwy konta przechowywanego we wbudowanym magazynie haseł za pomocą którego zalogowano się do systemu, c) przesyłanych plików między maszyną zewnętrznego dostawcy a zarządzanym zasobem, d) nagrania z sesji (sesje graficzne oraz okna konsoli), e) transkrypcji chatu, f) wszystkich uczestników sesji (osoby, które dołączały do sesji w trakcie jej trwania), g) listy zdarzeń (log) dotyczący pracy narzędzia uprzywilejowanego dostępu zdalnego. **Konfiguracja i instalacja agentów** 1. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi być przygotowany do masowej instalacji. 2. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi posiadać datę ważności, po upływie której niemożliwe będzie jego wykorzystanie. 3. Agent instalowany na zarządzanym zasobie musi być aktualizowany w sposób centralny z poziomu systemu uprzywilejowanego dostępu zdalnego. 4. System musi zapewniać możliwość określenia polityk aktualizacji agenta (możliwość definiowania co najmniej liczby jednocześnie aktualizowanych agentów oraz pasma przeznaczonego na aktualizację przez sieć).

	5. System musi zapewnić możliwość zdefiniowania akcji zbierania dodatkowych danych na temat zdalnego hosta przez agenta, bez konieczności nawiązywania sesji (przynajmniej w zakresie zużycia CPU, nazwy zalogowanego użytkownika, zajętości dysku). **Wbudowany magazyn haseł** 1. System musi posiadać wbudowaną funkcjonalność magazynu poświadczeń (przechowywanie nazw kont i haseł, ukrywanie widoczności haseł przed zewnętrznymi dostawcami). 2. System musi umożliwiać dodawanie kont wykorzystywanych do zdalnego logowania co najmniej poprzez: a) wprowadzenie ręczne z poziomu interfejsu konfiguracyjnego narzędzia, b) wyszukanie i import z Active Directory, z możliwością automatycznej zmiany haseł na takich kontach. c) możliwość zintegrowania pobierania poświadczeń z systemu PAM (przynajmniej jednego), poświadczenia muszą być prezentowane w kontekście zasobu, do którego łączy się zewnętrzny dostawca (przy nawiązywaniu sesji musi być możliwość wyboru poświadczeń występujących wyłącznie na danym zasobie). 3. Użycie poświadczeń przez zewnętrznych dostawców 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: a) edycji grup zasobów w zakresie nadawania uprawnień dostępowych do zasobów dla zewnętrznych dostawców oraz uprawnień do edycji tych zasobów (zabronienie możliwości edycji zasobów w systemie uprzywilejowanego dostępu zdalnego), b) edycji i tworzenia nowych poświadczeń w magazynie

	haseł oraz do przyznawania uprawnień dla zewnętrznych dostawców do możliwości wykorzystania tych poświadczeń, c) generowania i podglądu raportów w tym nagrań z sesji, d) możliwości zapraszania do sesji dodatkowych użytkowników, e) możliwości odebrania lub nadania uprawnień do realizowania sesji z wykorzystaniem instalowanych agentów, serwerów proxy, protokołu RDP lub SSH. f) możliwości definiowania białych lub czarnych list poleceń w sesjach uruchamianych w konsoli.
Zakres wdrożenia:	1. Inicjalizacja oprogramowania w środowisku Zamawiającego 2. Konfiguracja i instalacja agentów (5 sztuk na systemach Windows i Linux) lub utworzenie elementów połączeniowych (5 sztuk RDP oraz SSH) 3. Instalacja konsol dostępowych oraz ich konfiguracja 4. Skonfigurowanie integracji z domeną na potrzeby logowania do dostarczanego systemu 5. Konfiguracja i instalacja jump point jeśli jest dostępny 6. Konfiguracja sejfu haseł, import i tworzenie kont zarządzanych 7. Utworzenie do 3 grup użytkowników i nadanie uprawnień (role administratorzy, wnioskujący – firma zewnętrzna, pracownicy domowi) oraz skonfigurowanie uprawnień 8. Utworzenie polityk dla sesji 9. Testy odbiorcze konfiguracji 10. Opracowanie dokumentacji powdrożeniowej oraz instrukcji używania systemu dla użytkowników końcowych

<u>Część nr 3 -</u> Narzędzie do repozytorium kodu źródłowego

Opis oprogramowania	**Narzędzie do repozytorium kodu źródłowego**
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 50 użytkowników; 2. Licencja musi zawierać prawo do instalacji na własnym serwerze. 3. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji.
Cechy oprogramowania	1. Oprogramowanie musi posiadać interfejs użytkownika dostępny przez przeglądarkę internetową; 2. Oprogramowanie musi posiadać funkcjonalność narzędzia kontroli wersji kodu źródłowego, 3. Oprogramowanie musi posiadać funkcjonalność narzędzia repozytorium kodu źródłowego, dokumentów, witryn i innych plików; 4. Oprogramowanie musi posiadać możliwość przeglądania kodu źródłowego, dokumentów, witryn i katalogu innych dokumentów; 5. Oprogramowanie musi posiadać możliwość zarządzania prawami dostępu do publikowanych materiałów; 6. Oprogramowanie musi posiadać możliwość zakładania nieograniczonej liczby prywatnych repozytoriów dla każdego z użytkowników; 7. Oprogramowanie musi posiadać możliwość automatycznego generowania plików README na podstawie plików podobnych do plików Markdown;

	8. Oprogramowanie musi posiadać funkcjonalność narzędzia do śledzenia problemów (Issue tracking); 9. Oprogramowanie musi posiadać możliwość budowania oprogramowania; 10. Oprogramowanie musi posiadać możliwość śledzenia zmian w komponentach i wersjach oprogramowania; 11. Musi istnieć możliwość logowania do serwera SYSLOG.
Inne wymagania	1. Oprogramowanie musi być dostarczone jako przedłużenie obecnej licencji na dotychczas posiadanym koncie lub dopuszczalne jest alternatywne rozwiązanie z migracją danych w najnowszej dostępnej wersji; 2. Oprogramowanie musi posiadać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania; 3. Oprogramowanie musi posiadać dostępność interfejsu REST API; 4. Oprogramowanie musi posiadać oprogramowanie oparte na Git; 5. Oprogramowanie musi posiadać możliwość integracji z oprogramowaniem do śledzenia błędów i zarządzania projektem opisanym w niniejszym projekcie, w zakresie pozwalającym na śledzenie i edytowanie błędów i problemów, powiązań pomiędzy problemami a kodem źródłowym; 6. Oprogramowanie musi posiadać możliwość instalacji oprogramowania na serwerze pracującym pod kontrolą systemu operacyjnego Linux; 7. Oprogramowanie musi posiadać możliwość integracji z systemami kontroli wersji (minimum z: Subversion, Mercurial, Git); 8. Oprogramowanie musi zapewniać możliwość integracji z Narzędzia do śledzenia błędów oraz zarządzania projektem

Część nr 4 - Części komputerowe

L.P.	Nazwa	Sztuk	Specyfikacja
1	Dysk 240GB 2,5”, SATA SSD	20	Typ: SSD SATA Typ obudowy: 2,5'' Pojemność dysku: 240 GB Interfejs: Serial ATA III; Maks. szybkość odczytu: 540 MB/s Maks. szybkość zapisu: 500 MB/s
2	Dysk 480 GB, 2,5 „ SATA SSD	15	Typ: SSD SATA; Typ obudowy: 2,5"; Pojemność dysku: 480 GB; Interfejs: Serial ATA III; Maks. szybkość odczytu: 540 MB/s; Maks. szybkość zapisu: 460 MB/s;
3	Dysk 1 TB, 2,5 „ SATA SSD	2	Typ: SSD SATA; Typ obudowy: 2,5"; Pojemność dysku: 1 TB; Interfejs: Serial ATA III; Maks. szybkość odczytu: 560 MB/s; Maks. szybkość zapisu: 530 MB/s;
4	Dysk M2	2	Pojemność: 500 GB Wersja M2: PCI-E x4 Gen4 NVMe Interfejs: M.2 Format M2: 2280 Prędkość Odczytu Sekwencyjnego: 3600MB/s

			Prędkość Zapisu Sekwencyjnego: 2000MB/s
5	Dysk 4 TB, 3,5”; SATA; typ HDD	1	Typ: HDD Pojemność dysku: 4 TB Interfejs: Serial ATA III Typ obudowy: 3.5" Rozmiar bufora: 256 MB Prędkość obrotowa: 5900 obr./min.
6	Dysk 480 GB 2,5” SSD zewnętrzny	2	Typ: SSD Rodzaj: zewnętrzny; Typ obudowy: 2,5"; Pojemność dysku: 500 MB; Interfejs: USB 3.2 - typ C Maks. szybkość odczytu: 1050 MB/s Maks. szybkość zapisu: 1000 MB/s
7	Pamięć	10	Rodzaj pamięci: DDR 2; Typ pamięci: DIMM; Przeznaczenie: Komputer PC; Pojemność: 4 GB (2x2); Moduły w zestawie: 2 x 2 GB; Obsługiwane systemy operacyjne Windows: Tak Dopuszczalny produkt używany w stanie :działające
8	Pamięć	6	Rodzaj pamięci: DDR 3; Typ pamięci: DIMM; Przeznaczenie: Komputer PC; Pojemność: 8 GB; Moduły w zestawie: 1 x 8 GB. Częstotliwość szyny pamięci : 1600 Mhz CAS latency (CL): 11 Pamięć niebuforowana: Tak Radiator: nie Obsługiwane systemy operacyjne Windows: Tak
9	Pamięć	8	Rodzaj pamięci: DDR 4; Typ pamięci: DIMM; Przeznaczenie: Komputer PC; Pojemność: 16 GB; Moduły w zestawie: 2 x 8 GB. Częstotliwość szyny pamięci : 3600 Mhz CAS latency (CL): 17 Pamięć niebuforowana: Tak Radiator: tak Obsługiwane systemy operacyjne Windows: Tak
10	Pamięć	2	Rodzaj pamięci: DDR 4 Typ pamięci: SO-DIMM; Przeznaczenie: Laptop; Pojemność: 32 GB; Moduły w zestawie: 1 x 32 GB. Prędkość zegara pamięci:3200 Mhz CAS latency (CL): 22 Obsługiwane systemy operacyjne Windows: Tak
11	Pamięć	4	Rodzaj pamięci: DDR 4; Typ pamięci: DIMM; Przeznaczenie: Komputer PC; Pojemność: 32 GB; Moduły w zestawie: 2 x 16 GB.

			Częstotliwość szyny pamięci : 3600 Mhz CAS latency (CL): 16 Pamięć niebuforowana: Tak Radiator: tak Obsługiwane systemy operacyjne Windows: Tak
12	Pamięć	4	Rodzaj pamięci: DDR 3 Typ pamięci: SO-DIMM; Przeznaczenie: Laptop; Pojemność: 8 GB; Moduły w zestawie: 1 x 8 GB. Prędkość zegara pamięci:1600 Mhz CAS latency (CL): 11 Obsługiwane systemy operacyjne Windows: Tak
13	Procesor + płyta główna	2	Procesor: Wynik procesor osiąga w teście PassMark Performance Test co najmniej 34,663punktów w Passmark CPU Mark. Dostępny w załączonym pliku: PassMark - CPU Benchmarks - List of Benchmarked CPUs.pdf Płyta główna: Kompatybilna z wybranym procesorem spełniająca co najmniej: Standard płyty: ATX Obsługiwana pamięć: DDR4 Rodzaj obsługiwanej pamięci : DIMM (do PC) Typ obsługiwanej pamięci: 2133,2400,2666,2933,3000,3200,3300,3333,3400,3466,3600,3666,3733,3800,3866,4000,4133,4266,4300,4400 Mhz Ilość gniazd pamięci: 4 szt. Maks. pojemność pamięci: 128 GB Złącza PCI-E (liczba slotów): • 3 x PCI-Express x16 Złącza dla dysków i napędów : 4 x Serial ATA III Złącza na tylnym panelu: • 1 x Display Port • 1 x HDMI • 1 x RJ45 • 1 x USB 3.2 (Gen2) typ C • 2 x USB 3.2 (Gen1) • 5 x USB • Audio Złącza na płycie głównej: • 1 x Audio • 1 x gniazdo M.2 • 1 x USB 3.2 (Gen1) • 1 x USB 3.2 (Gen2) typ C • 2 x gniazdo M.2 (PCIe 4.0) Wtyczka zasilania: ATX 24pin Zintegrowana karta sieciowa: tak - 2.5 Gigabit Ethernet Zintegrowana karta dźwiękowa: tak

14	Zasilacz	2	Moc: co najmniej 600 W Standard: ATX Ilość wentylatorów: 1 Układ PFC: Aktywny Złącza: • CPU 4+4 (8) pin - 1 szt. • PCI-E 2.0 6+2 (8) pin - 2 szt. • MOLEX 4-pin - 3 szt. • SATA - 5 szt. • EPS12V 24-pin - 1 szt. Zabezpieczenia: • Przeciwprzeciążeniowe (OPP) • Termiczne (OTP) • Przeciwprzepięciowe (OVP) • Przeciwzwarciowe (SCP) • Przed zbyt niskim napięciem (UVP)
15	Zasilacz	2	Moc: co najmniej 850 W Standard: ATX Ilość wentylatorów: 1 Układ PFC: Aktywny Złącza: • CPU 4+4 (8) pin - 2 szt. • PCI-E 2.0 6+2 (8) pin - 6 szt. • MOLEX 4-pin - 6 szt. • SATA - 16 szt. • EPS12V 20+4 (24) pin - 1 szt. • FDD - 1 szt. Zabezpieczenia: • Przeciwprzeciążeniowe (OPP) • Termiczne (OTP) • Przeciwprzepięciowe (OVP) • Przeciwzwarciowe (SCP) • Przed zbyt niskim napięciem (UVP) Typ okablowania: Modularny
16	Mysz	20	Typ: optyczna; Interfejs: USB; Liczba przycisków: 3 szt.; Liczba rolek: 1 szt.; Rozdzielczość (dpi): 1000 dpi; Typ transmisji bezprzewodowej: radiowy; Podświetlenie: nie; Cechy dodatkowe: odbiornik USB niewielkich rozmiarów; Sposób zasilania: baterie; Typ baterii: AA; Zasięg: ok 10 m, Gwarancja: 2 lata, Co najmniej 12 miesięczna żywotność akumulatora (podana przez producenta). Inteligentny tryb uśpienia w celu oszczędzania baterii, Łączność : 2,4 GHz,

17	Mysz	10	Typ: optyczna; Interfejs: USB; Liczba przycisków: 3 szt.; Liczba rolek: 1 szt.; Rozdzielczość (dpi): 1000 dpi; Typ transmisji bezprzewodowej: radiowy; Podświetlenie: nie; Cechy dodatkowe: odbiornik USB niewielkich rozmiarów; Sposób zasilania: baterie; Typ baterii: AA; Zasięg: ok 10 m, Co najmniej gwarancja producenta: 2 lata, Co najmniej 18 miesięczna żywotność akumulatora (podana przez producenta). Inteligentny tryb uśpienia w celu oszczędzania baterii, Łączność : 2,4 GHz, Mysz dla praworęcznych z zakrzywionym uchwytem z gumy.
18	Komplet klawiatura i mysz	4	 Komplet : Gwarancja: 2 lata Mysz w komplecie: tak Łączność: bezprzewodowa Komunikacja bezprzewodowa: fale radiowe Przeznaczenie: do biura Klawiatura: Typ klawiatury: Wyspowa Klawisze numeryczne: tak Interfejs: USB (odbiornik) Mysz Typ urządzenia: mysz optyczna Liczba przycisków: 2 szt. Rolka przewijania: 1 szt.
19	Klawiatura	10	Typ klawiatury: tradycyjna Typ klawiszy: membranowe Klawisze numeryczne: tak Interfejs: USB (odbiornik)
20	Filtr prywatności	1	Filtr ma umożliwić: - idealne czytelny widok z przodu – całkowicie czarny ekran z boku - chronić ekran przed zadrapaniami i odciskami palców - redukcję odbicia na ekranie Sposób instalacji - za pomocą pasków dwustronnie klejących oraz umożliwiająca łatwy demontaż za pomocą bocznych przezroczystych listków Na laptopa : Dell Latitude 7420 14”
21	kabel HDMI 3M	15	Typ: kabel; Końcówka 1: HDMI

			Końcówka 2: HDMI Zastosowanie: KABEL DO MONITORA Długość: 3 m.
22	kabel HDMI 5M	5	Typ: kabel; Końcówka 1: HDMI Końcówka 2: HDMI Zastosowanie: KABEL DO MONITORA Długość: 5 m.
23	Kabel do monitora	3	Typ: kabel; Końcówka 1: HDMI M Końcówka 2: DVI(24+1) M Zastosowanie: KABEL DO MONITORA Długość: 1,5 m.
24	Kabel do monitora	4	Typ: kabel; Końcówka 1: HDMI M Końcówka 2: DVI(18+1) M Zastosowanie: KABEL DO MONITORA Długość: 3 m.
25	Kabel do monitora	5	Typ: kabel; Końcówka 1: DVI(18+1) M Końcówka 2: DVI(18+1) M Zastosowanie: KABEL DO MONITORA Długość: 1,8 m.
26	Kabel do monitora	10	Typ: kabel; Końcówka 1: HDMI M Końcówka 2: VGA M Zastosowanie: KABEL DO MONITORA Długość: 1,8 m.
27	Kabel do monitora	10	Typ: kabel; Końcówka 1: HDMI M Końcówka 2: DisplayPort M Zastosowanie: KABEL DO MONITORA Długość: 1,5 m.
28	Kabel do monitora	25	Typ: kabel; Końcówka 1: VGA M Końcówka 2: DisplayPort M Zastosowanie: KABEL DO MONITORA Długość: 1,8 m.
29	Kabel do monitora	10	Typ: kabel; Końcówka 1: DisplayPort M Końcówka 2: DisplayPort M Zastosowanie: KABEL DO MONITORA Długość: 1 m.
30	Karta sieciowa	3	Port1: USB-C Port2: RJ45 Ethernet Transfer danych: 10/100/1000Mbps, IEEE 802.3, 802.3u (10Base-T, 100Base-T) Rodzaj : zewnętrzna Rodzaj komunikacji: przewodowa Kompatybilny z Thunderbolt 3 Typ: Plug and Play Najnowszy interfejs USB3.1 Typ-C Kompatybilność: Windows 10
31	Stacja dokująca	4	Typ: Stacja dokująca Interfejs: USB 3.0

			Rodzaje wejść / wyjść • USB 2.0 - 2 szt. • USB 3.0 Typu-B - 1 szt. • USB 3.0 - 3 szt. • HDMI - 2 szt. • RJ-45 (LAN) - 1 szt. • DisplayPort - 1 szt. • Gniazdo słuchawkowe - 1 szt. • Wyjście audio - 1 szt. • DC-in (wejście zasilania) - 1 szt. Zasilanie: Sieciowe Dodatkowe informacje: Obsługa monitora Ultra HD 4K; Wake on LAN Dołączone akcesoria: Adapter HDMI-DVI; Kabel USB 3.0; Zasilacz sieciowy
32	Kabel	3	Typ: kabel; Końcówka 1: Micro USB Końcówka 2: USB Długość: 3 m.
33	Ładowarka USB	4	Rodzaj : ładowarka uniwersalna Przeznaczenie: smartfon z możliwością ładowania indukcyjnego Liczba zasilanych urządzeń: 3 Rodzaj wtyku, złącza : USB Napięcie wyjściowe (V) : USB1 - 5V/1A, USB2/USB3 - 5V/2.4A Zasilanie (V): 100 - 240 V Kabel na wyposażeniu nie Wtyczka: EU
34	Kieszeń HDD	3	Typ dysku: HDD Maks. rozmiar urządzeń: 2.5 cala Obsługiwane urządzenia: dyski twarde Interfejs urządzeń: SATA Interfejs obudowy: USB 3.0 Kable w komplecie: USB 3.0 Obsługiwane systemy operacyjne: Windows 10, Windows 7
35	Pendrive	15	Pojemność: 32 GB Interfejs urządzenia: USB Wersja USB: 3.2 Gen 1 (3.1 Gen 1) Prędkość odczytu USB 3.2 Gen 1 (3.1 Gen 1): 150 MB/s Obsługiwane systemy operacyjne Windows : • Windows 10 Education • Windows 10 Education x64 • Windows 10 Enterprise • Windows 10 Enterprise x64 • Windows 10 Home • Windows 10 Home x64 • Windows 10 Pro • Windows 10 Pro x64 • Windows 7 Enterprise • Windows 7 Enterprise x64 • Windows 7 Home Basic • Windows 7 Home Basic x64

			• Windows 7 Home Premium • Windows 7 Home Premium x64 • Windows 7 Professional • Windows 7 Professional x64 • Windows 7 Starter • Windows 7 Starter x64 • Windows 7 Ultimate • Windows 7 Ultimate x64 • Windows 8 • Windows 8 Enterprise • Windows 8 Enterprise x64 • Windows 8 Pro • Windows 8 Pro x64 • Windows 8 x64 • Windows Vista Business • Windows Vista Business x64 • Windows Vista Enterprise • Windows Vista Enterprise x64 • Windows Vista Home Basic • Windows Vista Home Basic x64 • Windows Vista Home Premium • Windows Vista Home Premium x64 • Windows Vista Ultimate • Windows Vista Ultimate x64 Zgodny z Mac: Tak Obsługiwane systemy operacyjne Mac: • Mac OS X 10.10 Yosemite • Mac OS X 10.11 El Capitan • Mac OS X 10.12 Sierra • Mac OS X 10.6 Snow Leopard • Mac OS X 10.7 Lion • Mac OS X 10.8 Mountain Lion • Mac OS X 10.9 Mavericks Obsługiwane operacyjne systemy komórkowe: Android
36	Pendrive	15	Pojemność: 64 GB Interfejs urządzenia: USB Type-A i Micro-USB Wersja USB: 3.2 Gen 1 (3.1 Gen 1) Prędkość odczytu USB 3.2 Gen 1 (3.1 Gen 1): 150 MB/s Obsługiwane systemy operacyjne Windows : • Windows 10 Education • Windows 10 Education x64 • Windows 10 Enterprise • Windows 10 Enterprise x64 • Windows 10 Home • Windows 10 Home x64 • Windows 10 Pro • Windows 10 Pro x64 • Windows 7 Enterprise • Windows 7 Enterprise x64 • Windows 7 Home Basic • Windows 7 Home Basic x64 • Windows 7 Home Premium

			• Windows 7 Home Premium x64 • Windows 7 Professional • Windows 7 Professional x64 • Windows 7 Starter • Windows 7 Starter x64 • Windows 7 Ultimate • Windows 7 Ultimate x64 • Windows 8 • Windows 8 Enterprise • Windows 8 Enterprise x64 • Windows 8 Pro • Windows 8 Pro x64 • Windows 8 x64 • Windows Vista Business • Windows Vista Business x64 • Windows Vista Enterprise • Windows Vista Enterprise x64 • Windows Vista Home Basic • Windows Vista Home Basic x64 • Windows Vista Home Premium • Windows Vista Home Premium x64 • Windows Vista Ultimate • Windows Vista Ultimate x64 Zgodny z Mac: Tak Obsługiwane systemy operacyjne Mac: • Mac OS X 10.10 Yosemite • Mac OS X 10.11 El Capitan • Mac OS X 10.12 Sierra • Mac OS X 10.6 Snow Leopard • Mac OS X 10.7 Lion • Mac OS X 10.8 Mountain Lion • Mac OS X 10.9 Mavericks Obsługiwane operacyjne systemy komórkowe: Android
37	Pendrive	15	Interfejs: USB 3.1 i USB-C Pojemność: 64 GB Maks. prędkość odczytu: 150 MB/s Obsługiwane systemy operacyjne: • Mac OS X 10.6 • MacOS X • Windows 10 • Windows 7 • Windows 8
38	Karta graficzna	3	Wynik wbudowanej karty graficznej w teście PassMark Performance Test co najmniej 7820 punktów w G3D Rating. W załączonym pliku: PassMark Software - Video Card (GPU) Benchmark Charts - Video Card Model List.pdf Rodzaje wyjść/wejść: 1 x wyjście HDMI 2 x Display Port

39	Karta graficzna	3	Wynik wbudowanej karty graficznej w teście PassMark Performance Test co najmniej 635 punktów w G3D Rating. W załączonym pliku: PassMark Software - Video Card (GPU) Benchmark Charts - Video Card Model List.pdf Rodzaje wyjść/wejść: - VGA - HDMI - DVI-D (dual link)
40	Stacja dokująca HDD	2	Dane techniczne: Włącznik na obudowie Wyjścia: USB mini 5pin , 2x USB 2.0 HUB, 5 Slotów kart pamięci Obsługiwane systemy operacyjne: Windows 2000/XP/VISTA, 7, MAC OS X Zasilanie: zewnętrzny zasilacz Wejście: 100-240V, 50/60Hz, 1.5A Obsługująca rodzaje kart: CF SLOT (Compact Flash Card): CF I / CF II / Extreme CF / Extreme III CF / ULTRA II CF / HS CF / MD MS SLOT (Memory Stick): MS / MS Duo / MS Pro / MS Pro Duo / MS MG / MS MG Pro / MS MG Duo / MS MG Pro Duo / Extreme MS Pro / Extreme III Ms Pro / Ultra II Ms Pro / HS MS MG Pro / HS MS MG Pro Duo / MS Rom / MS Select SD SLOT SD / SDHC / Mini SD / Extreme SD / Extreme III SD / Ultra II SD / MMC (Mulimedia Card) / MMC 2 / MMC 4.0 / RS MMC / HS RS MMC / MICRO SD (T FLASH) X-Memory SLOT: X-Memory Obsługująca wszystkie dyski twarde SATA(I, II, III)/IDE 2,5" oraz 3,5" bez względu na pojemność. Posiadająca: HUB 2 porty: 2 szybkie porty USB 2.0 z przepustowością do 480Mb/s, do których można podłączyć inne urządzenia USB. Umożliwiająca robienie kopii zapasowych wyznaczonych przestrzeni dyskowych przez wciśnięcie jednego przycisku.
41	Security Key	1	Interfejs: USB NFC: tak Szyfrowanie: RSA 2048 | RSA 4096 (PGP) | ECC p256 | ECC p384
42	Latarka-czołówka	3	Moc: 150 lumenów Ciężar: 86 g Wiązka: szeroka Zasilanie: 3 baterie AAA/R03 (dostarczane z czołówką) Kompatybilność: akumulatorki Ni-MH Certyfikacja: CE Wodoodporność: IP X4 (wodoodporny) Trzy tryby oświetlenia: bliski, do

			przemieszczania się, daleki. Gwarancja: 5 lat
43	Podstawka pod laptopa	5	Typ: podstawka chłodząca Wentylator: Wbudowany duży, cichy wentylator (125mm) Przyciski: do włączania i wyłączania Wielkość: dostosowany do rozmiaru komputera od 12" do 17" Podłączenie: zasilane przez odpinany kabel USB Dodatkowe parametry: możliwość ustawiania laptopa na 3 różne poziomy wyżej
44	Bateria do laptopa	1	Bateria do laptopa Dell Latitude E6430
45	Patchcord	30	Typ wtyk: RJ45 Kategoria: 6a Długość: 5m Rodzaj: nieekranowe Spełniające wymagania norm ISO/IEC 11801 class E oraz IEC60332-1.
46	Patchcord	30	Typ wtyk: RJ45 Kategoria: 6a Długość: 3m Rodzaj: nieekranowe Spełniające wymagania norm ISO/IEC 11801 class E oraz IEC60332-1.
47	Patchcord	30	Typ wtyk: RJ45 Kategoria: 6a Długość: 1m Rodzaj: nieekranowe Spełniające wymagania norm ISO/IEC 11801 class E oraz IEC60332-1.
48	Patchcord	30	Typ wtyk: RJ45 Kategoria: 6a Długość: 0,5 m Rodzaj: nieekranowe Spełniające wymagania norm ISO/IEC 11801 class E oraz IEC60332-1.
49	Moduł	20	10GBASE-T SFP+ Copper RJ-45 30m Transceiver Kompatybilne z Switch DELL PowerConect serii 8024F i 3548
50	Kabel	6	SFP-H10GB Passive Direct Attach Copper Twinax 10GBSFP+ Długość – 3M
51	Kabel	4	SFP-H10GB Passive Direct Attach Copper Twinax 10GBSFP+ Długość – 5M
52	Uchwyt do mocowania telewizora na ścianie	1	Musi być kompatybilny z posiadanym telewizorem : Hisense Smart TV Qled 4K A7 Series 55. Uchwyt musi posiadać możliwości: - regulacja nachylenia - obrotowe ramię

			- niewielka odległość od ściany (płaska konstrukcja) - korekcję przechyłu (niwelacja błędów montażowych)

Gwarancja 24 miesięcy.

Część nr 5 - Narzędzia do śledzenia błędów oraz zarządzania projektem

Opis oprogramowania	**Narzędzia do śledzenia błędów oraz zarządzania projektem**
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 100 użytkowników; 2. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji.
Cechy oprogramowania	1. Oprogramowanie musi udostępniać podstawowy interfejs użytkownika dostępny przez przeglądarkę internetową; 2. Oprogramowanie musi realizować funkcjonalność narzędzia do śledzenia zadań (issue tracking) 3. Oprogramowanie musi realizować funkcjonalność narzędzia do zarządzania błędami (Bug tracking); 4. Oprogramowanie musi zapewniać możliwość zarządzania wieloma różnymi projektami; 5. Oprogramowanie musi zapewniać wsparcie dla kompleksowego zarządzania projektem i metod typu Agile (Agile Project Management); 6. Oprogramowanie musi zapewniać możliwość dowolnej konfiguracji przepływu pracy (workflow); 7. Oprogramowanie musi pozwalać integracja z popularnymi platformami programistycznymi jak Eclipse, IntelliJ IDEA, Microsoft Visual Studio, Microsoft Visual Studio Code, JDeveloper, NetBeans, Zend Studio, inne; 8. Oprogramowanie musi zapewniać możliwość zarządzania błędami, właściwościami projektu, zadaniami, osiągnięciami lub innymi zagadnieniami; 9. Oprogramowanie musi zapewniać możliwość połączenia tworzonych zadań i zgłoszeń z kodem źródłowym, dostęp do kodu źródłowego; 10.Oprogramowanie musi zapewniać możliwość dodawania załączników; 11.Oprogramowanie musi zapewniać możliwość tworzenia nowych zadań za pośrednictwem przeglądarki, poczty elektronicznej oraz zintegrowanego środowiska programistycznego (IDE); 12.Oprogramowanie musi zapewniać możliwość szeregowania zadań, nadawania priorytetów; 13.Oprogramowanie musi zapewniać możliwość śledzenia zmian w komponentach i wersjach oprogramowania; 14.Oprogramowanie musi zapewniać możliwość generowania powiadomień członków zespołu projektowego z możliwością ich konfiguracji; 15.Oprogramowanie musi zapewniać możliwość tworzenia ról, poziomów uprawnień, grup użytkowników; 16.Oprogramowanie musi zapewniać możliwość tworzenia użytkowników, przydzielanie ról, poziomów uprawnień dla grup użytkowników; 17.Oprogramowanie musi zapewniać możliwość definiowania uprawnień dostępu z poziomu panelu;

	18.Oprogramowanie musi zapewniać możliwość synchronizacji katalogu użytkowników z systemem uwierzytelniania opisanym w poniższym dokumencie oraz LDAP; 19.Oprogramowanie musi zapewniać możliwość rejestracji historii aktywności użytkowników – dostęp do ostatnio otwartych zadań, projektów; 20.Oprogramowanie musi zapewniać możliwość wyszukiwania pełnotekstowego, filtrowania i raportowania; 21.Oprogramowanie musi zapewniać możliwość generowania zestawień i statystyk podsumowujących realizacje projektu; 22.Oprogramowanie musi zapewniać możliwość generowania dokumentów w formacie xls, xlsx, xlsm, doc,docx; 23.Oprogramowanie musi zapewniać możliwość wyświetlania podsumowań i raportów dla rozpoczętych projektów – ostania aktywność, kamienie milowe, logi zmian, mapy projektu, wykresy;
Inne wymagania	1. Oprogramowanie musi być dostarczone jako przedłużenie obecnej licencji Jira Software na dotychczas posiadanym koncie lub dopuszczalne jest alternatywne rozwiązanie z migracją danych w najnowszej dostępnej wersji; 2. Oprogramowanie musi zapewniać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania; 3. Oprogramowanie musi zapewniać możliwość integracji z narzędziem do repozytorium kodu źródłowego dostarczonym w niniejszym postępowaniu 4. Możliwość integracji z systemami kontroli wersji (minimum z: Subversion, Mercurial, Git); 5. Dostępność aplikacji mobilnej na system Android i IOS.

Część nr 6 - Kamera typ1

I	**Kamera typ1**	30 szt.
1.	Zastosowanie	kamera będzie wykorzystywana na potrzeby internetowych spotkań on-line
2.	ZASTOSOWANIE	Wewnętrzna
3.	INTERFEJSY	USB 2.0
4.	ROZDZIELCZOŚĆ KAMERY INTERNETOWEJ	1280 x 720
5.	OBSŁUGIWANE ROZDZIELCZOŚCI	1280×720
6.	FUNKCJA APARATU CYFROWEGO	Tak
7.	FUNKCJE KAMERY	Wbudowany mikrofon
8.	SYSTEM	Windows 7, Windows 8
9.	GWRANCJA	Producenta nie mniejsza niż 24 miesiące

Część nr 7 – SUBSKRYPCJA OPOGRAMOWANIA DO PRACY BIUROWEJ ONLINE

I. Przedmiot zamówienia.

1. Przedmiotem zamówienia jest:
   a. zakup subskrypcji oprogramowania do pracy biurowej online typu M365 EDU A3 FACULTY (lub równoważny),
   b. przedłużenie obecnie posiadanych subskrypcji. Zamawiający jest w posiadaniu subskrypcji: Power BI Pro FACULTY,

dla **Sieci Badawczej Łukasiewicz – Instytutu Technik Innowacyjnych EMAG** w ilościach zgodnych z Załącznikiem nr 1 do niniejszego OPZ – Zestawienie ilościowe przedmiotu zamówienia.

Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego, przy czym kryterium stosowanym do oceny równoważności jest spełnienie co najmniej tych samych cech, parametrów technicznych, funkcjonalnych i innych na poziomie co najmniej takim jak opisane w niniejszym dokumencie.

II. Oświadczenie Zamawiającego

1. Zamawiający informuje, iż na mocy ustawy z dnia 21.02.2019 r. o Sieci Badawczej Łukasiewicz, zostało utworzone Centrum Łukasiewicz i instytuty Sieci.

   Na mocy powyższej ustawy Art. 98 Instytutu Technik Innowacyjnych EMAG w Katowicach stał się instytutem Sieci. Instytut Sieci jest państwową osobą prawną powołaną do prowadzenia badań naukowych i prac rozwojowych. Celami Sieci są: prowadzenie badań aplikacyjnych i prac rozwojowych, transfer wiedzy oraz wdrażanie wyników badań naukowych i prac rozwojowych do gospodarki, wspieranie polityki gospodarczej państwa, prowadzenie działalności mającej na celu kształtowanie świadomości społecznej na temat zaawansowanych technologii.

   Na mocy ustawy z dnia 21.02.2019 r. o Sieci Badawczej Łukasiewicz dokonano zmiany w przepisach w Ustawie z dnia 20.07.2018 r. Prawo o szkolnictwie wyższym i nauce, stanowiącej Załącznik d do Ekspertyzy, z zgodnie z Art. 7 ust. 6b) instytuty działające w ramach Sieci Badawczej Łukasiewicz również tworzą „System szkolnictwa wyższego i nauki".
2. Zamawiający oświadcza, że obecnie wykorzystuje rozwiązanie oparte o platformę Microsoft 365 oraz jej elementy takie jak konta użytkowników w ramach dostawcy tożsamości Azure Active Directory (zarówno w zakresie dostępu Online jak i integracji z urządzeniami końcowymi w postaci laptopów), skrzynki pocztowe (zwykłe i współdzielone) oraz listy dystrybucyjne oparte o platformę Exchange Online, platformę przechowywania/współdzielenia plików opartą o rozwiązania OneDrive oraz SharePoint jak również platformę komunikacji Teams, oraz platformy Planner i Forms. Pracownicy oraz współpracownicy Zamawiającego są obecnie przeszkoleni z wykorzystania powyższych systemów.
3. W przypadku zaproponowania rozwiązania równoważnego do platformy Microsoft 365 Zamawiający wymaga wdrożenia w postaci:
   a. Zapewnienia rozwiązania pozwalającego na integrację z istniejącym systemem Azure Active Directory (wraz z ewentualnymi kosztami utrzymania systemu) lub przeprowadzenie migracji na nową platformę w zakresie wszystkich użytkowników i grup,
   b. Przeprowadzenia migracji wszystkich skrzynek pocztowych (użytkowników oraz współdzielonych) na nowy system wraz z danymi (korespondencja, kalendarze indywidualne i grupowe). Migracja powinna być przeprowadzona w sposób niewpływający na pracę Zamawiającego z uwzględnieniem jego specyfiki (praca z partnerami w wielu strefach czasowych), w terminie do 14 dni kalendarzowych od dnia zawarcia umowy. Zamawiający

dopuszcza przerwę w działaniu usługi poza wyznaczonymi godzinami aktywności, jednak nie dopuszcza całkowitej niedostępności poczty elektronicznej mogącej skutkować utratą danych w trakcie migracji.

c. Przeniesienia danych z osobistych dysków OneDrive z zachowaniem przypisania uprawnień.

d. Przygotowanie dokumentacji wprowadzającej do platformy dla nowych pracowników i przekazanie w formie elektronicznej nie później niż 3 dni przed szkoleniem, o którym mowa w punkcie e,

e. Przeszkolenie pracowników Zamawiającego z zasad działania nowej platformy; Zamawiający wymaga zrealizowania co najmniej dwóch szkoleń grupowych przeprowadzonych online, w terminie uzgodnionym z Zamawiającym nie później niż 10 dni roboczych po dostawie licencji objętych pierwszym zamówieniem:

- jedno szkolenie – dla użytkowników licencji,
- drugie szkolenie – dla administratorów.

4. Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego, przy czym kryterium stosowanym do oceny równoważności jest spełnienie co najmniej tych samych cech, parametrów technicznych, funkcjonalnych i innych na poziomie co najmniej takim jak opisane w Załączniku nr 2 do OPZ.
5. Zgodnie z art. 99 ust. 5 Pzp Ustawy w każdym przypadku, gdzie wskazano lub użyto w niniejszym dokumencie oraz załącznikach znaków towarowych, patentów lub pochodzenia, źródła materiałów należy rozumieć, że dopuszcza się stosowanie materiałów równoważnych o porównywalnych (nie gorszych) parametrach technicznych, eksploatacyjnych i użytkowych niż te, które wskazano. Ponadto zgodnie z art. 101 ust 1 pkt. 3 Pzp Ustawy ilekroć w niniejszym dokumencie lub załącznikach w opisie przedmiotu zamówienia wskazano określone normy, aprobaty, specyfikacje techniczne lub systemy odniesienia należy rozumieć, że Zamawiający dopuszcza rozwiązania równoważne.

III. Wymagania szczegółowe przedmiotu zamówienia.

1. Zamawiający wymaga, aby Wykonawca dostarczył najnowsze wersje Produktów o ile opis przedmiotu zamówienia nie stanowi inaczej.
2. Warunki użytkowania oprogramowania muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi lub serwerami (np. w przypadku wymiany lub uszkodzenia sprzętu).
3. Oferowane produkty i usługi muszą zapewniać posiadanie powszechnie uznanych i rozpowszechnionych standardów i normatywów potwierdzonych aktualnymi wynikami niezależnych audytów, w szczególności:
   - ISO 27001,
   - ISO 27002,
   - ISO 27017,
   - ISO 27018 lub równoważne,
   - SOC 2, SOC 3 lub równoważne,
   - Open Authentication Standard – OAuth lub równoważne.
4. Oferowane subskrypcje usług hostowanych muszą zapewniać:

- Wszystkie elementy usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę zarządzania tożsamością użytkowników;
- Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym), w trybie 24/7;
- Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy;
- Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO lub równoważnymi;
- Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi;
- Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego;
- Dostępność mechanizmu uwierzytelnienia wieloskładnikowego - uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej;
- Wbudowana usługa zarządzania tożsamością użytkowników musi umożliwiać realizację uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory;
- Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”;
- Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików;
- Ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day;
- Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich;
- Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN);
- Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS;
- Przynajmniej dwa niezależne od siebie, równorzędne ośrodki przetwarzania danych. Centra przetwarzania świadczące usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego;
- Dostęp do usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS;
- Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych;
- Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług;
- Gwarancję braku dostępu do danych Zamawiającego na platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody Zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy platformy;

5. Dostarczane subskrypcje oprogramowania będące przedmiotem niniejszego zamówienia, muszą gwarantować prawo instalacji najnowszej wersji oprogramowania, dostępnych w trakcie trwania umowy.
6. Zamawiający dopuszcza oferowanie produktów o szerszej niż opisana funkcjonalności.
7. W związku z możliwością zwiększenia liczby użytkowników systemów w trakcie trwania umowy, Zamawiający wymaga zaoferowania licencjonowania gwarantowanego przez Producenta produktów, umożliwiającego w okresie trwania umowy instalację dodatkowych licencji z zamawianego zakresu produktów z rozliczaniem się post factum w maksymalnych ilościach wskazanych w Załączniku nr 1 do OPZ.

8. Wykonawca zapewni dostęp do spersonalizowanej strony Producenta dedykowanej dla Zamawiającego pozwalającej upoważnionym osobom ze strony Zamawiającego na:

- Pobieranie zakupionego oprogramowania,
- Dostęp do usług,
- Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania,
- Sprawdzanie liczby zakupionych/aktywnych Produktów w wykazie zakupionych Produktów,

9. Wykonawca zobowiązany jest zapewnić pełne wsparcie w tym dokonanie stosowanych zgłoszeń m.in. do Producenta w czasie trwania umowy przy czynnościach Zamawiającego związanych z pracami polegającymi na przeniesieniu Tenantu Zamawiającego (posiadanych subskrypcji oprogramowania) do Tenantu Centrum Łukasiewicza.
10. Zamawiający wymaga udzielenia uprawnień na stronie Producenta oraz dostępu do kluczy licencyjnych w terminie do 5 dni od podpisania umowy.
11. W okresie obowiązywania umowy oferowana usługa będzie przechowywać dane oraz umożliwiać uprawnione przetwarzanie danych, które pozostają wyłączną własnością Zamawiającego. Po zakończeniu okresu obowiązywania umowy w przypadku podjęcia decyzji o baraku jej kontynuacji, usługa będzie przechowywać dane Zamawiającego, które zostały w niej zapisane, na koncie o ograniczonej funkcjonalności przez 90 dni od daty wygaśnięcia lub wypowiedzenia subskrypcji w celu umożliwienia ich odzyskania. Po upływie tego 90-dniowego okresu przechowywania konto związane z subskrypcją usługi zostanie wyłączone, a dane Zamawiającego zostaną usunięte.
12. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym.
13. Jeżeli nowa wersja produktu zawierać będzie bardziej restrykcyjne prawa do używania niż wersja, która była aktualna na dzień złożenia oferty, te bardziej restrykcyjne prawa do używania nie będą miały zastosowania do korzystania z tego Produktu przez Zamawiającego.

IV. Termin realizacji i rozliczania przedmiotu zamówienia.

1. Dostarczenie/udostępnienie nowych licencji musi się odbyć w przypadku licencji M365 EDU A3 FACULTY przed wygaśnięciem obecnie posiadanych licencji O365 EDU A3 FACULTY, oraz Power BI Pro FACULTY przed wygaśnięciem obecnie posiadanych licencji Power BI Pro FACULTY.

2. Zamawiający wyraża zgodę na dokonywanie płatności miesięcznych na potrzeby wyrównania dat obowiązujących subskrypcji jak również różnego czasu zamawiania nowych subskrypcji.
3. W zakresie nowych subskrypcji Zamawiający będzie składał zamówienie, w którym zostanie wskazany tenant właściwy dla przypisania subskrypcji.

V. Oświadczenia i zobowiązania Wykonawcy.

1. Wykonawca oświadcza, że przedmiot umowy w chwili jego dostarczenia będzie kompletny i wolny od wad, zarówno fizycznych jak i prawnych oraz że nie będzie obciążony jakimikolwiek prawami przysługującymi osobom trzecim.
2. Wykonawca oświadcza, że dostarczone w ramach umowy licencje są dopuszczone do obrotu gospodarczego na terytorium Rzeczpospolitej Polskiej.
3. **Wykonawca potwierdza, że jest uprawniony przez właściciela licencji do realizacji przedmiotu zamówienia i posiada oświadczenie producenta upoważniające go do odsprzedaży subskrypcji w ramach programu CSP lub równoważnego, <u>które to oświadczenie Wykonawca przedłoży Zamawiającemu przed czynnością podpisania umowy[1].</u>**

[1] W przypadku braku przedłożenia oświadczenia, Zamawiający uzna, że Wykonawca uchyla się od podpisania umowy.

4. Wszystkie produkty wymienione w niniejszym opisie przedmiotu zamówienia muszą pochodzić bezpośrednio od Producenta Oprogramowania Microsoft lub równoważnego.
5. Subskrypcje oprogramowania mają być dostarczone bezpośrednio od Producenta, niedopuszczalne jest uczestniczenie w łańcuchu dostawy osób trzecich.
6. Jeżeli realizacja zamówienia będzie wymagać zawarcia przez Zamawiającego dodatkowej umowy z jakimkolwiek innym podmiotem, Wykonawca będzie zobowiązany zapewnić, aby postanowienia takiej umowy były zgodne ze wszystkimi warunkami i wymogami wynikającymi z dokumentów dotyczących zamówienia. W szczególności, nie dopuszcza się, aby postanowienia te narzucały na Zamawiającego jakiekolwiek inne obowiązki niż określone w dokumentach dotyczących zamówienia lub ograniczały jego uprawnienia wynikające z tychże dokumentów.
7. Oferowane Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).
8. Subskrypcje wchodzące w skład przedmiotu zamówienia, winny być dostarczone w polskiej wersji językowej (PL) z możliwością zmiany na inne języki [w tym obowiązkowo na język angielski (EN)].
9. Zawarte w opisie przedmiotu zamówienia wymagania i zobowiązania Wykonawcy – o ile nie zastosowano wyłączenia – dotyczą zarówno Wykonawcy, który dostarczy produkty Microsoft, jak i Wykonawcy, który dostarczy produkty równoważne.

VI. Aktualizacja i wsparcie techniczne

1. Zamawiający wymaga świadczenia usługi wsparcia technicznego przez cały okres ich używania.
2. Nośniki oprogramowania (jeśli występują) powinny być objęte 90-dniową gwarancją.
3. Oprogramowanie musi być objęte wsparciem Producenta w szczególności w zakresie: pomocy we wdrożeniu, instalacji, codziennym użytkowaniu, zarządzaniu, utrzymaniu subskrypcji oraz usuwaniu powstałych usterek.
4. Poziom dostępności Subskrypcji nie może być mniejszy niż 99,9% w skali miesiąca.
5. Licencjonowanie musi uwzględniać prawo do bezpłatnej instalacji udostępnionych przez producenta oprogramowania (Producenta) uaktualnień, poprawek krytycznych i opcjonalnych w okresie trwania subskrypcji.

VII. Warunki równoważności dla produktów równoważnych – szczegółowa specyfikacja techniczno-eksploatacyjna i cech użytkowych oprogramowania:

1. W przypadku zaoferowania oprogramowania równoważnego do obowiązków Wykonawcy należy:
    a. dostarczenie pełnych wersji Produktu na wszystkie zasoby Zamawiającego z zachowaniem kompatybilności dla oprogramowania wdrożonego oraz używanego u Zamawiającego (oprogramowanie narzędziowe, specjalistyczne, dedykowane aplikacje) przy całkowitym spełnianiu warunków, o których mowa w niniejszym dokumencie.
    b. udowodnienie, że funkcjonalność oferowanego oprogramowania jest równoważna w stosunku do oprogramowania wskazanego w niniejszym opisie przez Zamawiającego. Ocena produktu równoważnego odbędzie się w trybie badania i oceny ofert na podstawie dokumentów i dowodów przedłożonych Zamawiającemu. Polegać będzie na wykazaniu pełnej współpracy oferowanego oprogramowania z systemami i oprogramowaniem posiadanym przez Zamawiającego, poprawnym współdziałaniu ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego, nie powodującym zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego Zamawiającego.
    c. Pełna implementacja Produktów na istniejących konfiguracjach środowiska produkcyjnego i testowego.
2. Równoważny produkt musi bez zakłóceń współpracować z posiadaną przez Zamawiającego infrastrukturą sprzętową oraz wykorzystywanym oprogramowaniem i systemami, do których należą: serwery, laptopy, komputery stacjonarne, urządzenia drukujące, urządzenia sieciowe, systemy Windows, oprogramowanie Microsoft, środowisko wirtualizacyjne, telefony oraz smartfony. Na

Wykonawcy oferującym produkty równoważne spoczywa odpowiedzialność w zakresie prawidłowego działania zaoferowanych produktów w środowisku pracy użytkowników produktów po stronie Zamawiającego.

3. Wykonawca musi zapewnić warunki i zakres usługi wsparcia Producenta dla oferowanych produktów.
4. Wykonawca musi wykazać, że funkcjonalność każdego produktu równoważnego spełnia opisane funkcjonalności
.
5. Wykonawca musi zapewnić, że produkty równoważne są kompatybilne i będą w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem systemowym, aplikacyjnym i użytkowym, eksploatowanym i obsługiwanym przez Zamawiającego.
6. Wykonawca musi zapewnić, warunki i zakres usługi asysty wsparcia technicznego dla Produktów Microsoft lub równoważnych.
7. Wykonawca zobowiązany jest pokryć koszty zmiany w zakresie produktów i rozwiązań Microsoft na produkty i rozwiązania równoważne, konieczne do właściwego działania całego środowiska sprzętowo-programowego Zamawiającego. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.
8. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Dodatkowo w przypadku błędnego działania środowiska po instalacji rozwiązania równoważnego, Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ.

Załącznik nr 1

Lista posiadanych licencji przez zamawiającego

Producent	**Nazwa oprogramowania**	**Liczba posiadanych produktów**
Microsoft	O365 EDU A3 FACULTY	150
Microsoft	Power BI Pro FACULTY	6

Zestawienie ilościowe przedmiotu zamówienia - zakupu i odnowienia licencji

Producent	**Nazwa oprogramowania**	**Liczba produktów do zakupienia/przedłużenia**
Microsoft	M365 EDU A3 FACULTY - Zakup	200
Microsoft	Power BI Pro FACULTY - odnowienie	6

Załącznik nr 2

Warunki równoważności produktów.

Usługa poczty elektronicznej on-line musi spełniać następujące wymagania:

Usługa musi umożliwiać:

a. obsługę poczty elektronicznej,
b. zarządzanie czasem,
c. zarządzania zasobami
d. zarządzanie kontaktami i komunikacją.

Usługa musi dostarczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:

e. Zarządzania użytkownikami poczty,
f. Wsparcia migracji z innych systemów poczty,
g. Wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
h. Wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty. Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:
   - Posiadanego oprogramowania Outlook (2010, 2013, 2016, 2019),
   - Przeglądarki (Web Access),
   - Urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 30 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa funkcji takich jak tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Edge, Firefox i Safari,
- Współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy,
- Bezpieczny dostęp z każdego miejsca, w którym jest dostępny Internet.

Usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:
   a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych,
   b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata,
   c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami,
   d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia,
   e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
2. Funkcjonalność wspierająca pracę grupową:

a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie.

b. Możliwość określenia terminu wygaśnięcia wiadomości. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.

c. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze.

d. Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania.

e. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań Obsługa list i grup dystrybucyjnych.

f. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej i wiadomości błyskawicznych.

g. Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu.

h. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.

i. Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami.

j. Funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności.

k. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.

l. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów.

m. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.

3. Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:

a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu.

b. Archiwizację oraz definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników.

c. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych.

d. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne.

e. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów.

f. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie

ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.

g. Integracja z usługami zarządzania dostępem do treści (ADRMS) pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania.

h. Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.

i. Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.

j. Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.

4. Wsparcie dla użytkowników mobilnych:

   a. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu. Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem online i off-line w zależności od stanu połączenia z serwerem.

   b. Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.).

   c. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone.

   d. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej.

   e. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, Microsoft Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.

   f. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

Usługa portalu on-line musi realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy:

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych.
2. Zarządzanie strukturą portalu i treściami www.
3. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści.
4. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej.
5. Tworzenie repozytoriów wzorów dokumentów.
6. Tworzenie repozytoriów dokumentów.
7. Wspólną, bezpieczną pracę nad dokumentami.
8. Wersjonowanie dokumentów (dla wersji roboczych).
9. Organizację pracy grupowej.
10. Wyszukiwanie treści.
11. Dostęp do danych w relacyjnych bazach danych.
12. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.

13. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

Serwery portali muszą posiadać następujące cechy dostępne bezpośrednio jako wbudowane właściwości
produktu:

1. Interfejs użytkownika:
   a. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
   b. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów.
   c. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego.
   d. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
2. Projektowanie stron:
   a. Wbudowane intuicyjne narzędzia projektowania wyglądu stron.
   b. Wsparcie dla ASP.NET, Apache, C#, Java i PHP.
   c. Możliwość osadzania elementów iFrame w polach HTML na stronie.
3. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
   a. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili.
   b. Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów.
   c. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do Maili.
   d. Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego.
   e. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services.
   f. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

Usługa portalu on-line musi mieć wbudowaną funkcjonalność udostępniania użytkownikom komponentów pakietu biurowego on-line dostępnego przez przeglądarkę. Pakiet biurowy on-line musi spełniać następujące wymagania:

1. Wymagania odnośnie interfejsu użytkownika:
   a. Pełna polska wersja językowa interfejsu użytkownika.
   b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
   a. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247).

3. Pakiet biurowy on-line musi zawierać:
    a. Edytor tekstów,
    b. Arkusz kalkulacyjny,
    c. Narzędzie do przygotowywania i prowadzenia prezentacji,
    d. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.
4. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
    b. Wstawianie oraz formatowanie tabel,
    c. Wstawianie oraz formatowanie obiektów graficznych,
    d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego,
    e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
    f. Automatyczne tworzenie spisów treści,
    g. Formatowanie nagłówków i stopek stron,
    h. Sprawdzanie pisowni w języku polskim,
    i. Śledzenie zmian wprowadzonych przez użytkowników,
    j. Określenie układu strony (pionowa/pozioma),
    k. Wydruk dokumentów,
    l. Pracę na dokumentach utworzonych przy pomocy Microsoft Word z zapewnieniem konwersji wszystkich elementów i atrybutów dokumentu,
    m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
5. Arkusz kalkulacyjny musi umożliwiać:
    a. Tworzenie raportów tabelarycznych.
    b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
    c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
    d. Wyszukiwanie i zamianę danych.
    e. Wykonywanie analiz danych przy użyciu formatowania warunkowego,
    f. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
    g. Formatowanie czasu, daty i wartości finansowych z polskim formatem,
    h. Zapis wielu arkuszy kalkulacyjnych w jednym pliku,
    i. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,
    j. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,
6. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    a. Przygotowywanie prezentacji multimedialnych, które będą:
        - Prezentowanie przy użyciu projektora multimedialnego,
        - Drukowanie w formacie umożliwiającym robienie notatek,
        - Zapisanie jako prezentacja tylko do odczytu,
    b. Nagrywanie narracji i dołączanie jej do prezentacji,

c. Opatrywanie slajdów notatkami dla prezentera,
d. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
e. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
f. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
g. Możliwość tworzenia animacji obiektów i całych slajdów,
h. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,
i. Zgodność z formatami plików utworzonych za pomocą oprogramowania Microsoft PowerPoint.

Usługa serwera komunikacji wielokanałowej on-line (SKW) wspomagająca wewnętrzną i zewnętrzną komunikację ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

1. Bezpieczną komunikację głosową oraz video,
2. Przesyłanie wiadomości błyskawicznych (tekstowych),
3. Możliwość organizowania telekonferencji,
4. Możliwość współdzielenia dokumentów w trakcie spotkań on-line (zdalnych).

W połączeniu z funkcjami aplikacji klienckich usługa ma zapewnić uprawnionym użytkownikom:

1. Wymianę informacji z możliwością wyboru i zmiany dostępnego kanału komunikacji, tj. wiadomości tekstowych (chat), rozmowy (przekazywanie dźwięku), wideo rozmowy (przekazywanie dźwięku i obrazu), współdzielenie lokalnych pulpitów w systemach Windows oraz współdzielenie dokumentów z możliwością przejmowania kontroli i edycji przez uprawnionych uczestników.
2. Kontakt poprzez wymienione kanały w modelu jeden do jednego, jeden do wielu, telekonferencji (kontakt interakcyjny wielu osób) oraz udostępniania dźwięku i obrazu dla wielu osób w sieci intranet lub Internet.
3. Możliwość oceny jakości komunikacji głosowej i wideo.
4. Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze katalogowej oraz definiowania opisów użytkowników zewnętrznych w tym użytkowników wybranych bezpłatnych komunikatorów i użytkowników sieci telefonii przewodowej i komórkowej.
5. Dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką SKW lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub specjalizowanych urządzeń stacjonarnych typu telefon IP, kamera dookólna czy duże monitory lub projektory.
6. Dostępny kliencki sprzęt peryferyjny różnych producentów posiadający potwierdzenie zgodności z SKW przez producenta SKW.
7. Dostępność informacji o statusie dostępności użytkowników na liście adresowej (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności, w tym składowanych w usłudze katalogowej.
8. Możliwość grupowania kontaktów w komunikacji tekstowej z możliwością konwersacji typu jeden-do-jednego, jeden-do-wielu i możliwością rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat.
9. Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.
10. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.
11. Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).

12. Możliwość nagrywania telekonferencji przez uczestników.
13. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
14. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
15. Wbudowana funkcjonalność mostka konferencyjnego MCU.
16. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
17. Kodowanie video H.264,
18. Wsparcie dla adresacji IPv4 i IPv6,
19. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
20. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników,
21. Możliwość szyfrowania połączeń,
22. Dostępność uczestniczenia w telekonferencjach poprzez przeglądarkę dla użytkowników z poza organizacji, zaproszonych do udziału w telekonferencji z funkcjami:
    a. Dołączania do telekonferencji.
    b. Szczegółowej listy uczestników.
    c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
    d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
    e. Dostępu do udostępnianych plików.
    f. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji.
23. Dostępność aplikacji klienckiej usługi SKW (komunikatora) z funkcjonalnością:
    a. Listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielania grup kontaktów typu ulubione lub ostatnie.
    b. Historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
    c. Wsparcia telekonferencji:
        - Dołączania do telekonferencji,
        - Szczegółowej listy uczestników,
        - Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,
        - Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
        - Głosowania,
        - Udostępniania plików i pulpitów,
        - Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji.
24. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
25. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.
26. Wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji SKW z wybranymi systemami poczty elektronicznej i portali intranet/Internet oraz usługą katalogową Active Directory. Wynikiem takiej integracji mają być następujące funkcje i cechy systemu opartego o SKW dostępne dla użytkowników posiadających odpowiednie uprawnienia nadane przez administratorów:

a. Wykorzystanie domenowego mechanizmu uwierzytelnienia w oparciu o usługę katalogową, jej profile użytkowników i ich grup oraz realizację fizyczną pojedynczego logowania (single signon) dla uprawnionego dostępu do usług SKW.

b. Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).

c. Współdziałanie mechanizmów SKW z pocztą głosową, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:

- Uruchamiania funkcji komunikacyjnych SKW z wybranych interfejsów klienta poczty elektronicznej, składników pakietu biurowego czy portalu.
- Dostępności w tych interfejsach danych o statusie obecności innych użytkowników (np. w nagłówkach poczty elektronicznej, czy listach użytkowników portalu.
- Możliwość planowania rozmów czy telekonferencji bezpośrednio poprzez zaproszenia w kalendarzu klienta poczty elektronicznej, generujące link do spotkania on-line.

Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 1 TB dla każdego użytkownika. Repozytorium musi umożliwiać użytkownikom pakietów biurowych na:

1. Traktowanie go, jako własnego dysku.
2. Synchronizację zawartości wybranego folderu ze stacji roboczej do repozytorium przypisanego danemu użytkownikowi na bazie niezaprzeczalnego uwierzytelnienia.
3. Synchronizację zawartości repozytorium z wieloma urządzeniami w ramach uprawnień użytkownika – właściciela repozytorium.

Subskrypcja pakietu biurowego

Usługa hostowana on-line musi zawierać subskrypcję pakietu biurowego spełniającego następujące wymagania:

Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit.
2. Wymagania odnośnie interfejsu użytkownika:
   a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
   b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
   c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
3. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w poprzednich wersjach pakietów biurowych, jeśli takowe istnieją.
4. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
   a. posiada kompletny i publicznie dostępny opis formatu,
   b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247),
   c. umożliwia kreowanie plików w formacie XML,

5. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
6. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
7. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
8. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
9. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a. Edytor tekstów,
   b. Arkusz kalkulacyjny,
   c. Narzędzie do przygotowywania i prowadzenia prezentacji,
   d. Narzędzie do tworzenia drukowanych materiałów informacyjnych,
   e. Narzędzie do tworzenia i pracy z lokalną bazą danych,
   f. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
   g. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR,
   h. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
10. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c. Wstawianie oraz formatowanie tabel.
    d. Wstawianie oraz formatowanie obiektów graficznych.
    e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    g. Automatyczne tworzenie spisów treści.
    h. Formatowanie nagłówków i stopek stron.
    i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
    j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
    k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
    l. Określenie układu strony (pionowa/pozioma).
    m. Wydruk dokumentów.
    n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
    o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 i nowszych z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
    p. Zapis i edycję plików w formacie PDF.
    q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco.

s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.

11. Arkusz kalkulacyjny musi umożliwiać:

a. Tworzenie raportów tabelarycznych.

b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.

c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.

d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).

e. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.

f. Wyszukiwanie i zamianę danych.

g. Wykonywanie analiz danych przy użyciu formatowania warunkowego.

h. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.

i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.

j. Formatowanie czasu, daty i wartości finansowych z polskim formatem.

k. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.

l. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.

m. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).

n. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 i nowszych, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.

o. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

12. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

a. Przygotowywanie prezentacji multimedialnych, które będą:

i. Prezentowane przy użyciu projektora multimedialnego,

ii. Drukowane w formacie umożliwiającym robienie notatek.

b. Zapisanie jako prezentacja tylko do odczytu.

c. Nagrywanie narracji i dołączanie jej do prezentacji.

d. Opatrywanie slajdów notatkami dla prezentera.

e. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.

f. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.

g. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.

h. Możliwość tworzenia animacji obiektów i całych slajdów.

i. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.

j. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania Microsoft PowerPoint 2007 i nowszymi.

13. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
    a. Tworzenie i edycję drukowanych materiałów informacyjnych.
    b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
    c. Edycję poszczególnych stron materiałów.
    d. Podział treści na kolumny.
    e. Umieszczanie elementów graficznych.
    f. Wykorzystanie mechanizmu korespondencji seryjnej.
    g. Płynne przesuwanie elementów po całej stronie publikacji.
    h. Eksport publikacji do formatu PDF oraz TIFF.
    i. Wydruk publikacji.
    j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
14. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
    a. Tworzenie bazy danych przez zdefiniowanie:
        - Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
        - Relacji pomiędzy tabelami.
        - Formularzy do wprowadzania i edycji danych.
        - Raportów.
        - Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych.
        - Tworzenie bazy danych przy użyciu zdefiniowanych szablonów.
        - Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.
15. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
    a. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory.
    b. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
    c. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
    d. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
    e. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
    f. Automatyczne grupowanie poczty o tym samym tytule.
    g. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
    h. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
    i. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
    j. Zarządzanie kalendarzem.
    k. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
    l. Przeglądanie kalendarza innych użytkowników.
    m. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.

n. Zarządzanie listą zadań.

o. Zlecanie zadań innym użytkownikom.

p. Zarządzanie listą kontaktów.

q. Udostępnianie listy kontaktów innym użytkownikom.

r. Przeglądanie listy kontaktów innych użytkowników.

s. Możliwość przesyłania kontaktów innym użytkowników.

t. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

16. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:

a. Pełna polska wersja językowa interfejsu użytkownika.

b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

c. Dostępność aplikacji na platformie Windows 7 lub wyższych oraz OSX 10 lub wyższych,

d. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

e. Możliwość obsługi tekstowych wiadomości błyskawicznych w modelu jeden do jeden i jeden do wielu.

f. Możliwość komunikacji głosowej i video w modelu jeden do jeden i jeden do wielu.

g. Obsługa telekonferencji SKW:

- Dołączania do telekonferencji,
- Szczegółowej listy uczestników,
- Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,
- Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
- Głosowania,
- Udostępniania plików i pulpitów,
- Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,

h. Możliwość zmiany kanału komunikacji z pośrednictwem wiadomości błyskawicznych do połączenia głosowego i/lub wideo w ramach pojedynczej, otwartej w aplikacji sesji (bez konieczności przełączania się pomiędzy aplikacjami).

i. Lista adresowa wraz ze statusem obecności, opisem użytkowników SKW, zdjęciami użytkowników, listą dostępnych do komunikacji z nimi kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji oraz wydzielania grup kontaktów typu ulubione lub ostatnie.

j. Status obecności, dający możliwość ręcznego ustawiania statusu (dostępny, zajęty, nie przeszkadzać, z dala od komputera, niedostępny), automatycznej synchronizacji z jego aktywnością w systemie operacyjnym stacji roboczej, a w przypadku instalacji wybranych systemów poczty elektronicznej – dostępu do informacji o dostępności użytkownika na bazie wpisów do jego kalendarza.

k. Możliwość rozszerzania listy adresowej o zewnętrznych użytkowników wraz z informacjami opisowymi i kontaktowymi.

l. Historia ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień.

m. Integracja ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.

n. Definiowanie i konfiguracja urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

o. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.

p. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.

q. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Usługi bezpieczeństwa

Usługi bezpieczeństwa wbudowane w produkt muszą pozwalać na:

a. Zarządzanie prawami dostępu do dokumentów i poczty elektronicznej tworzonych w Usłudze poprzez ich szyfrowanie i nadawanie praw odczytu, edycji, wydruku dla konkretnych użytkowników Usługi lub grup użytkowników Usługi.

b. Wykrywanie słów kluczowych w przesyłanych wiadomościach i sygnalizowanie potencjalnego wycieku informacji.

c. Możliwość ograniczania przedziału czasowego uprawnionego dostępu użytkowników do informacji.

d. Możliwość stosowania wymogu wieloskładnikowego uwierzytelniania.

e. Możliwość przydzielania uprawnień administratorom w oparciu o role.

f. Możliwość kontroli przepływu danych w ramach usługi repozytorium dokumentów/SKW oraz usługi poczty elektronicznej w oparciu o mechanizmy DLP (Data Loss Prevention)

g. Możliwość zaawansowanej analizy zagrożeń w usłudze w czasie rzeczywistym

h. Możliwość wykorzystania uwierzytelniania wieloskładnikowego (MFA) przy logowaniu do usługi będącej przedmiotem zamówienia oraz aplikacji internetowych Zamawiającego wykorzystujących SSO/SAML.

i. Możliwość tworzenia zasad dostępu warunkowego dla usług i dynamiczne przydzielanie polityk bezpieczeństwa zależnie od przypisanej do użytkownika roli.

j. Możliwość samodzielnej zmiany hasła przez użytkowników z wykorzystaniem witryny internetowej.

k. Możliwość przypisywania licencji poszczególnym użytkownikom.

l. Możliwość logowania się użytkowników i zarządzania stacjami roboczymi bez konieczności bezpośredniego podłączenia do lokalnego kontrolera domeny Zamawiającego. Zarządzanie stacjami roboczymi musi obejmować między innymi:

   - Zarządzanie ochroną antywirusową.
   - Zarządzanie aktualizacjami.
   - Zarządzanie licencjami posiadanego oprogramowania firmy Microsoft.
   - Konfigurowanie polityk zabezpieczeń.

Usługi analizy danych

Usługi analizy danych wbudowane w produkt muszą umożliwiać:

a. Konfigurowanie on-line kokpitów informacyjnych wizualizujących wyniki analiz danych.

b. Gotowe mechanizmy podłączania różnego rodzaju danych strukturalnych, semi-strukturalnych i niestrukturalnych.

c. Korzystanie z gotowych algorytmów i modeli analizy oraz budowa własnych modeli w języku R.

d. Możliwość instalacji bramy w środowisku on-premises, która umożliwia eksport danych do systemu online.

Usługi zarządzania urządzeniami oraz tożsamością użytkowników

Subskrypcja usługi zarządzania urządzeniami oraz tożsamością użytkowników musi spełniać następujące wymagania:

a. Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy.

b. Zagwarantowanie poziomu dostępności na poziomie min 99,9%.

c. Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm, w tym zgodności z normami ISO 27017 i 27018 lub równoważnymi.

d. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO.

e. Możliwość skalowania usługi z ustalonymi kosztami takiego skalowania.

f. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi.

g. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego.

h. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.

i. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.

j. Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione".

k. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych, l. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową,
pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN).

m. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS.

n. Mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.

o. Możliwość wykorzystania Right Management Services (RMS) - ochronę treści na urządzeniach mobilnych.

p. Portal klasy self-service dla użytkowników mobilnych pozwalający na zdalny reset haseł i zarządzanie przynależnością do grup security w usłudze katalogowej.

q. Podniesienie poziomu bezpieczeństwa dostępu do aplikacji webowych – poprzez uwierzytelnianie wieloskładnikowe (np. poprzez jednorazowe hasła SMS).

r. Prawo do korzystania z rozwiązania klasy on-premise, który służy do zaawansowanego zarządzanie tożsamością w organizacji.

s. Automatyczna klasyfikacja treści dokumentów (przechowywanych na zasobach plikowych, bibliotekach lub transportowanych poprzez system pocztowy) zgodnie z definiowanymi wzorcami,

t. Wykorzystanie klasyfikacji danych do dynamicznego aplikowanie restrykcji związanych z dostępem do informacji zapobiegające niekontrolowanemu wyciekowi informacji.

u. Bezpieczna wymiana plików wewnątrz organizacji oraz z zewnętrznymi odbiorcami niezależnie od typu pliku, posiadanego urządzenia (PC lub urządzenie mobilne Windows Phone, Android, iOS) lub przynależności do organizacji, umożliwiające granularną kontrolę dostępu do poufnych informacji i wymuszenie ustalonych polityk ochrony informacji.

v. Możliwość wykorzystania telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS lub specjalizowanych aplikacji, potwierdzających tożsamość użytkownika

podczas dostępu do aplikacji webowych pozwalające na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia, lub z poza sieci lokalnej.

w. Możliwość pracy na prywatnych urządzeniach użytkowników zapewniający bezpieczny i kontrolowany dostęp do danych i aplikacji, w możliwością wydzielenia i usunięcia danych służbowych z urządzenia.

x. Jednokrotne logowanie (single sign-on) w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika, przy zachowaniu niezaprzeczalności działań.

y. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwalający na redukcję ilości zgłoszeń działów wsparcia.

z. Automatyczne przepływy pracy i reguł biznesowych pozwalające przyspieszenie procesów i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie ustalonych polityk i procedur).

aa. Ochrona danych poprzez wykrywanie i mapowanie ról biznesowych pozwalające na audyt i kontrolę zgodności realizacji uprawnień użytkowników z ustalonymi politykami oraz ciągłą weryfikację stanu bezpieczeństwa systemów.

bb. Zarządzanie urządzeniami mobilnymi pozwalające na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwiające zdalne kasowanie danych firmowych lub całego urządzenia.

Część nr 8 - Słuchawki typ1

I	**Słuchawki typ1**	55 szt.
1.	Zastosowanie	słuchawki wykorzystywane będą na potrzeby internetowych spotkań on-line
2.	Łączność	Przewodowa
3.	Złącze komunikacyjne	USB
4.	Regulacja głośności	Tak
5	Aktywna redukcja szumów	Tak
6.	Typ słuchawek	Nauszne
7.	Gwarancja	24 miesiące
Słuchawki cechy:		
8.	Min. pasmo przenoszenia	42 Hz
9.	Maks. pasmo przenoszenia	17000 Hz
10.	Czułość	95 dB/mW
Mikrofon cechy:		
11.	Min. pasmo przenoszenia	90 Hz
12.	Maks. pasmo przenoszenia	15000 Hz

<u>Część nr 9 -</u> OPOGRAMOWANIE DO SKANOWANIA WEBAPLIKACJI, PODATNOŚCI, OCHRONY ACTIVE DIRECTORY I ZASOBÓW CHMUROWYCH ORAZ DO MIERZENIA CYBER RYZYKA (250 szt)

Opis oprogramowania	**Oprogramowanie do skanowanie webaplikacji, podatności, ochrony Active Directory i zasobów chmurowych oraz do mierzenia cyber ryzyka**
Warunki licencji	1. Licencja na ma umożliwiać skanowanie co najmniej 250 serwerów, webaplikacji i kontenerów oraz w ramach tej ilości instalację agentów do skanowania systemów operacyjnych na stacjach do których skaner nie ma bezpośredniego dostępu 2. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji.
Cechy oprogramowania	**Kluczowe funkcjonalności:** 1. Skanowanie podatności i zarządzanie nimi 2. Skanowanie web aplikacji 3. Ochrona Active Directory 4. Mierzenie cyber ryzyka 5. Monitorowanie zasobów chmurowych **Funkcjonalności skanowania i zarządzania podatnościami:** 1. Architektura systemu musi składać się z systemu centralnego zarządzania oraz skanerów podłączonych do tego systemu pochodzących od tego samego producenta co system centralnego zarządzania. 2. System centralnego zarządzania musi być dostarczony w modelu chmurowym. 3. Skanery podłączone do systemu centralnego zarządzania muszą być dostępne jako oprogramowanie instalowane na systemie operacyjnym Red Hat 6/7, Fedora 25, FreeBSD 10/11,Cent OS 6/7, Windows Server 2016/2019, Windows 7/8/10, MAC OS 10.13, 10.14, 10.15 lub jako maszyna wirtualna dla środowiska Vmware lub Hyper-V. 4. Zarządzanie systemem musi odbywać się za pomocą przeglądarki, nie dopuszcza się zarządzania za pomocą dodatkowo instalowanej aplikacji na komputerze administratora. 5. System centralnego zarządzania musi w ramach licencji zezwalać na podłączenie nieograniczonej liczby skanerów producenta systemu zarządzania. 6. Skanery podłączone do systemu centralnego zarządzania muszą mieć możliwość wykonywania skanowania bez uwierzytelnienia oraz za pomocą uwierzytelnienia do systemu skanowanego. 7. GUI system centralnego zarządzania musi pozwalać na ściągnięcie logów ze zdalnego skanera. 8. System centralnego zarządzania musi prezentować informacje o użyciu licencji w formie wykresu z historią. 9. System centralnego zarządzania musi posiadać możliwość podłączenia się do środowisk chmurowych takie jak Amazon AWS,

	Microsoft Auzre, Google Cloud Platfrom w celu inwentaryzacji systemów oraz ich skanowania. 10. W ramach skanowania z uwierzytelnieniem musi istnieć możliwość uwierzytelnienia przynajmniej za pomocą poniższych metod: a) Hasło b) Klucz SSH c) Kerberos, d) LM Hash e) NTLM Hash f) zastosowanie integracji z Liberman g) zastosowanie integracji z BeyondTrust h) zastosowanie integracji z LibermanThycotic Secret Server i) zastosowanie integracji z Cyberark j) zastosowanie integracji z Arcon, k) zastosowanie integracji z Hashicorp Vault l) Certyfikat m) DB2 n) File Transfer Protocol (FTP) o) Microsoft SQL Server p) MySQL Server q) Oracle r) Post Office Protocol (POP) s) PostgreSQL t) Simple Network Management Protocol (SNMP) 11. W przypadku niektórych metod uwierzytelnienia do systemu skanowanego musi istnieć możliwość automatycznego podniesienia uprawnień zwykłego użytkownika do uprawnień użytkownika uprzywilejowanego co najmniej dla systemów Cisco oraz systemów Linuxowych. 12. Wykryte podatności muszą posiadać szybkie odniesienie do otwartych baz podatności, takich jak: a) Bugtraq b) MSFT c) CVE d) BID e) OSVDB ID 13. Musi być możliwość ustawienia harmonogramu automatycznego skanowania. 14. System musi posiadać możliwość tworzenia okien czasowych, w których skanowanie nie może rozpocząć się dla określonych przez administratora systemów. 15. System centralnego zarządzania musi być dostarczony z kilkoma wzorcami polityk skanowania jak również musi istnieć możliwość zbudowania polityki skanowania od podstaw. 16. W ramach budowy polityki skanowania system musi zezwala na wybranie podatności jakie będą sprawdzane podczas skanowania. 17. System musi posiadać rozbudowany moduł do przeszukiwania wyników skanowania. Musi istnieć możliwość przeszukiwania wyników co najmniej za pomocą filtrów takich jak: Adres IP, Poziom niebezpieczeństwa, CVE ID, CVSS Score w wersji 2, CVSS Vector w wersji 2, CVSS Score w wersji 3, CVSS Vector w wersji 3,nazwa AWS

	EC2, Azure VM ID , Googl Cloud Zone, dostępny exploit, narzędzie do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas), data opublikowania patch dla danej podatności, port, protokół, data opublikowania podatności, data zauważenia po raz pierwszy podatności dla systemu, data kiedy ostatni raz widziana była podatność dla systemu, przydział do określonej grupy systemów, MS Bulletin ID. 18. System centralnego zarzadzania musi pozwala na zapisywania filtrów przeszukiwania danych. 19. System musi pozwalać na eksport informacji o podatnościach w formatach, CVS, JSON. 20. System musi prezentować aktualizacje, które przyczyniają się do jak najszybszego obniżenia ryzyka w organizacji. 21. System musi posiadać swój własny mechanizm przyznawania ocen dla danej podatności od 0 do 10 na podstawie własnego modelu uczenia maszynowego oraz działu ekspertów, którzy monitorują zagrożenia w Internecie, między innymi w dark necie. 22. Administrator systemu musi mieć możliwość zaakceptowania danego ryzyka oraz zmiany poziomu niebezpieczeństwa związanego z daną podatnością. 23. System musi umożliwiać tworzenie tagów, które można przypisać ręcznie lub automatycznie i używane są podczas przeszukiwania wyników skanowania. 24. System musi być dostarczony z gotowymi wzorcami raportów. 25. Wybór systemów do skanowania musi być oparty o adresy IP, zakres adresów IP, podsieci adresów IP, grup systemów opartych o tagi, nazw domenowych. 26. Producent musi dostarczyć gotowe wzorce widoków (ang. Dashboard) do systemu centralnego zarządzania podatnościami. 27. Administrator systemu musi mieć możliwość budowania widoków od podstaw używając co najmniej takich elementów jak: tabela, wykres kołowy, wykres słupkowy. 28. Administrator do tworzenia widoków musi mieć możliwość użycia co najmniej wymienionych filtrów: adres IP, Poziom niebezpieczeństwa, CVE ID, CVSS Score w wersji 2, CVSS Vector w wersji 2, CVSS Score w wersji 3, CVSS Vector w wersji 3, dostępny exploit, narzędzie do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas), data opublikowania patch'a dla danej podatności, port, protokół, data opublikowania podatności, data pierwszy raz zauważenia podatności dla systemu, data kiedy ostatni raz widziana była podatność dla systemu, przyodział do określonej grupy systemów, Ms Bulletin ID. 29. Rozwiązanie musi integrować się z zewnętrznymi dostawcami systemów MDM, co najmniej: AirWatch MDM, Apple Profile Manager, Good MDM, MobileIron, Microsoft Intune, Blackberry UEM, MaaS360. 30. System musi mieć możliwość integracji z systemami zarządzania aktualizacjami w celu sprawdzenia czy wynik ze skanowania pokrywa się z informacjami z tych systemów. System musi integrować się co najmniej z takimi systemami jak: Microsoft SCCM,

	Microsoft WSUS, IBM Tivoli Endpoint Manager, Red Hat Satellite Server, Red Hat Satellite 6 Server, Symantec Altiris. 31. System musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA. 32. System musi umożliwiać tworzenie swoich własnych wzorców sprawdzania zgodności z regulacjami bez konieczności kontaktu z producentem, jak również muszą być udostępnione informacje w jaki sposób można budować swoje własne wzorca sprawdzania zgodności ze standardami przyjętymi w firmie. 33. Musi być możliwość wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów Windows, Unix, Vmware, Cisco, Fortigate, Oracle, DB2, MySQL, SQL Server, PostgreSQL, Juniper. 34. System musi posiadać opisane integracje min. z systemami ServiceNow, Jira, Splunk, IBM Qradar, Microsoft Azure,Google Cloud Security Command Center, Amazon Web Services. W przypadku implementacji z Jirą w środowisku lokalnym wymagane jest aby integracja była wykonana za pomocą dodatku do systemu Jira. 35. Możliwości skryptowania / API dla systemu centralnego zarządzania. **Funkcjonalności skanowania web aplikacji:** 1. Dostępny jako rozwiązanie typu cloud wraz z dostępnymi skanerami w rożnych częściach świata – minimum 14 skanerów podpiętych do systemu zarządzania umieszczonych na świecie zaimplementowanych przez producenta. 2. Zarządzanie przez przeglądarkę webową bez konieczności instalowania systemu zarządzania na własnym środowisku. 3. Możliwość skanowania web aplikacji niedostępnych od strony Internetu, za pomocą dodatkowego silnika skanującego, który łączy się z systemem zarządzania znajdującym się w chmurze. 4. Skaner lokalny służący do skanowania aplikacji webowych lokalnie musi być dostarczony jako maszyna wirtualna dla systemu Vmware lub Hyper-V. 5. Możliwość uwierzytelnienia do web aplikacji za pomocą cookie, użycie skryptu selenium, klucza API, login/form, certyfikatu, poświadczeń użytkownika w Kerberosie. 6. Posiadać przynajmniej dla jednej przeglądarki internetowej dodatek pozwalający w łatwy sposób utworzyć plik selenium w celu uwierzytelnienia do aplikacji webowej. 7. Pozwalać na skonfigurowanie polityki, w ramach której określone jest jakie podatności będą sprawdzane. 8. Możliwość skanowania aplikacji webowej co najmniej przez 99 godzin w ramach jednego uruchomionego skanu. 9. Pozwalać na skonfigurowanie jakie URL mają być poddane analizie jak również musi być opcja, w której skanowane są wskazane URL oraz podstrony tych URL'i. 10. Prezentować jakie dokładnie zapytanie http zostało przesłane ze skanera do analizowanej aplikacji webowej i jaka dokładnie została przesłana odpowiedź. 11. Możliwość określenia maksymalnej liczby przekierowań (redirect). 12. Możliwość ustawienia maksymalnej liczby skanowanych URL,

	natomiast skaner nie może mieć odgórnego limitu dla maksymalnej liczby skanowanych URL. 13. Możliwość określenia maksymalnego zagnieżdżenia analizowanej aplikacji webowej, natomiast skaner nie może mieć odgórnego limitu dla maksymalnego zagnieżdżenia. 14. Możliwość konfiguracji nagłówka http, który będzie użyty podczas wysyłania zapytań do skanowanej aplikacji webowej. 15. Możliwość ustawienia maksymalnej liczby jednoczesnych połączeń. 16. Możliwość ustawienia maksymalnej liczby zapytań http na sekundę. 17. Możliwość określenia jakie URL nie będą brane pod uwagę podczas skanowania. 18. Możliwość określenia jakie elementy na stronie nie będą brane pod uwagę podczas skanowania. 19. Generowanie mapy aplikacji webowej z informacją jakie URL zostały znalezione podczas skanowania. 20. Rysowanie linii trendu w czasie dla podatności związanych z aplikacjami webowymi. 21. Informowanie czy zalogowanie do analizowanej aplikacji webowej udało się czy nie. 22. Informowanie o wykrytej podatności z informacją jak ją wyeliminować. 23. Prezentowanie informacji, kiedy pierwszy raz dana podatność została zaobserwowana i kiedy ostatni raz dla skanowanej aplikacji webowej. 24. Informowanie o punktacji CVSSv2 i CVSSv3 dla wykrytej podatności. **Funkcjonalności narzędzia do mierzenia cyber ryzyka:** 1. Obliczanie ryzyka dla każdego systemu w organizacji w oparciu o informacje o podatnościach, prawdopodobieństwo użycia ich oraz innych wskaźników ryzyka takich jak min. krytyczność biznesowa atakowanego systemu. 2. Obliczanie automatyczne krytyczności każdego systemu w organizacji w oparciu o parametry stosowane przez system mierzenia ryzyka oraz możliwość nadania stopnia krytyczności systemowi ręcznie w skali od 1 -10. 3. Informacje o podatnościach pochodzące od tego samego producenta co system do obliczenia ryzyka. 4. Wizualizację trendu efektywności programu redukcji ryzyka. 5. Prezentację jakości dokonywanych skanów, która bierze pod uwagę minimum: częstotliwość skanowania systemów, czy skanowanie jest z uwierzytelnieniem czy nie, ilość użytych funkcji do wykrycia podatności, rekomendowane akcje w celu polepszenia jakości dokonywanych skanów w organizacji. 6. Porównanie min. parametrów związanych z efektywnością programu obniżenia ryzyka, jakości dokonywanych skanów do innych firm z tej samej branży. 7. Możliwość grupowania systemów w grupy pod kontem biznesowym. 8. Obliczania cyber ryzyka w organizacji w oparciu o kontekst biznesowy. 9. Listę rekomendowanych akcji, które zmniejszają cyber ryzyko w

	oparciu o decyzje biznesowe wraz z możliwością zagłębienia się w daną podatność, system w celu podjęcia bardziej efektywnej decyzji dotyczącej zmniejszenia ryzyka. 10. Prezentację informacji na temat usuniętych podatności min. w oparciu o czas pierwszego wykrycia podatności, czas od kiedy dostępny jest patch na daną podatność. **Funkcjonalności narzędzia do monitorowania bezpieczeństwa zasobów chmurowych:** 1. Możliwość integracji ze środowiskami chmurowymi AWS, Azure, GCP. 2. Wykrywanie błędów w konfiguracji i niezgodności z politykami w infrastrukturze chmurowej. 3. Możliwość monitorowania zmian w środowisku chmurowym. 4. Możliwość wykrywania podatności na instancjach EC2 w chmurze AWS bez implementacji skanerów. 5. Możliwość użycia gotowych wzorców zgodności z regulacjami dostarczonych przez producenta systemu jak również jest możliwość tworzenia swojego własnego wzorca polityk zgodności. 6. Możliwość integracji z systemami typu CI/CD min. Jenkins do wykrywania błędów w konfiguracji oraz podatności. 7. Możliwość integracji z narzędziami SCM min. GitHub, Bitbucket lub GitLab. 8. Możliwość integracji z takimi systemami jak Splunk, Jira, Slack, Terraform. 9. Możliwość ściągnięcia logów z lokalnego skanera kodu plików IaC. 10. Możliwość wykrywania różnic pomiędzy definicją IaC i tym co jest uruchomione w środowisku chmurowym. 11. Możliwość sprawdzenia klastra Kubernetes pod kontem zgodności ze zdefiniowanymi politykami. **Funkcjonalności narzędzia do ochrony i wykrywania ataków w Active Directory:** 1. Brak instalacji dodatkowego oprogramowania/agenta na Active Directory w celu integracji rozwiązania. 2. Możliwość zaimplementowania rozwiązania w środowisku lokalnym lub chmurowym. 3. Wykrywanie słabych punktów w konfiguracji Active Directory, które mogą zostać użyte przez atakujących. 4. Prezentowanie jakichkolwiek aktywności/zmian związanych z Active Directory w czasie rzeczywistym. 5. Rekomendowanie kroków w celu wyeliminowania słabych punktów w konfiguracji. 6. Tworzenie własnych dashboardów. 7. Wykrywanie niebezpiecznych relacji zaufania w środowisku Active Directory. 8. Wizualizowanie każdego zagrożenia na linii czasu.

	9. Łączenie zdarzeń związanych ze zmianami w Active Directory ze złośliwymi akcjami. 10. Szczegółowa analiza ataków na AD. 11. Prezentacja ścieżki ataku z konkretnego punktu do konkretnego systemu, wszystkich ścieżek ataku do konkretnego systemu. 12. Wykrywanie technik używanych podczas ataków min: a) DCShadow, b) Brute Force, c) Password Spraying, d) DCSync, e) Golden Ticket, f) NTDS Extraction. 13. Integracja z systemami typu SIEM/SOAR min. QRadar, Splunk, Phantom. 14. Powiazanie wykrytego incydentu z opisem MITRE ATT&CK.

<u>Część nr 10 –</u> TERMINALE DO INFRASTRUKTURY VDI – 8 SZT.

1	Wyświetlacz: Wyświetlacz bez obsługi dotykowej o przekątnej max. 14" i rozdzielczości min. FHD (1920 x 1080) przy min. 60 Hz z powłoką przeciwodblaskową, jasność min. 250 nitów, kamera/mikrofon
2	Pamięć: min. 2GB 1x2GB, 2400MHz DDR4 Memory – Kryterium Oceniane
3	Porty min: • 1 port USB Type-C™ 3.1 pierwszej generacji z obsługą standardów Power Delivery i DisplayPort 1.2 • 2 porty USB 3.0 • 1 port USB 2.0 z funkcją PowerShare • 1 port HDMI 2.0a do podłączenia zewnętrznego wyświetlacza 4K 60 Hz • 1 wyjście VGA • 1 gniazdo RJ-45 • 1 gniazdo audio • 1 złącze zasilania
	Klawiatura QWERTY
4	Monitor: dołączony do zestawu, kompatybilny z oferowanym terminalem mobilnym, tego samego producenta, o parametrach: • Zastosowanie: Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu, poczty elektronicznej oraz systemu SIMPLE.ERP • Przekątna ekranu: 24” • Rodzaj matrycy: LED, IPS • Rozdzielczość ekranu: 1920 x 1200 • Format obrazu: 16:10 • Częstotliwość odświeżania ekranu: 60Hz • Liczba wyświetlanych kolorów: 16,7 ml • Czas reakcji plamki: 5 ms – 8 ms • Kontrast: 1000:1 • Jasność: 300 cd/m² • Kąt widzenia pion: 178 °

	• Kąt widzenia poziom: 178 ° • Porty wejścia/wyjścia: DisplayPort x 1, HDMI x 1, USB 3.2 / USB 3.2 x 4, DVI x 1, VGA x 1 • Głośniki: nie • Pivot: tak • Wielkość plamki: 0,27mm • Możliwość montażu na ścianie: tak / Standard VESA 100x100 mm • Informacje dodatkowe: obrotowa podstawa, regulacja pochylania w pionie, regulacja wysokości • Klasa energetyczna: SDR D • Wyposażenie: instrukcja obsługi, kabel DisplayPort, kabel USB • Gwarancja: Producenta nie mniejsza niż 36 miesiący
6	Klawiatura i mysz: Dołączone do zestawy, kompatybilne z oferowanym terminalem mobilnym, o parametrach: Klawiatura: • Typ: Klasyczna; • Łączność: Bezprzewodowa; • Interfejs: 2,4 GHz, USB; • Klawisze: multimedialne / funkcyjne 8; • Kolor: Czarny; • Czas pracy na baterii: Do 2 lat; • Obsługiwane systemy: Windows; • Maksymalny zasięg: 10 m; • Dołączone akcesoria: 2 baterie typu AAA, Nanoodbiornik Myszka: • Typ: optyczna; • Interfejs: USB; • Liczba przycisków: 3 szt.; • Liczba rolek: 1 szt.; • Rozdzielczość (dpi): 1000 dpi; • Typ transmisji bezprzewodowej: radiowy; • Podświetlenie: nie; • Cechy dodatkowe: odbiornik USB niewielkich rozmiarów; • Sposób zasilania: baterie; • Typ baterii: AA; • Zasięg: ok 10 m, • Gwarancja: 2 lata, • Co najmniej 12 miesięczna żywotność akumulatora (podana przez producenta). • Inteligentny tryb uśpienia w celu oszczędzania baterii, • Łączność : 2,4 GHz,
	Stacja dokując: dołączona do zestawu, kompatybilna z oferowanym terminalem mobilnym, tego samego producenta, o minimum portach jak poniżej: • 1 x 3,5 mm minijack (Combo) • 2 x HDMI Type A • 1 x DisplayPort • 1 x RJ-45 (LAN) • 5 x USB 3.0 Type A
7	Dysk SSD SATA M.2 2230 Class 20 o pojemności min. 32 GB
8	Procesor min. 2 Core/4MB/2T/up to 2.6GHz/6W, kompatybilny z dostarczanym chipsetem

9	Łączność bezprzewodowa, minimum: • WiFi 802.11ac MU-MIMO 2x2 • Bluetooth w wersji 5
10	Wbudowana kamera internetowa z zasłoną obiektywu
11	Typ urządzenia: Mobilny terminal kliencki klasy Thin
12	Zasilanie: Zasilacz max 65 W
13	Masa: Waga max 2 kg
15	Gniazda min. • 1 gniazdo blokady klinowej Noble • 1 czytnik kart pamięci SD
16	Certyfikaty: - znak bezpieczeństwa „CE”, ISO9001:2000 producenta terminala, Terminal musi być zaprojektowany i wyprodukowany w całości przez jednego producenta.
17	System operacyjny: Dedykowany system do łączenia się do infrastruktury VDI Zamawiającego, bazującym na VMware Horizon, który ma mieć możliwość pełnej, automatycznej konfiguracji po podpięciu do sieci w której osiągalny jest serwer zarządzający systemami terminalowymi. Wynikiem automatycznej konfiguracji ma być możliwość zalogowania się do wirtualnej maszyny klienckie w infrastrukturze VDI
18	Gwarancja NBD na min. 12 miesięcy

<u>Część nr 11 -</u> ZINTEGROWANE ŚRODOWISKO PROGRAMISTYCZNE

Zintegrowane środowisko programistyczne musi:

1. Umożliwiać zintegrowaną obsługę języków Visual Basic, Visual C# i Visual C++, która pozwala na stosowanie różnych stylów programowania
2. Obsługiwać funkcje edytora, takie jak zmień i kontynuuj, które upraszczają cykl projektowania, tworzenia kodu i debugowania aplikacji,
3. Obsługiwać wdrażanie aplikacji klienckich z wykorzystaniem ClickOnce, dzięki której programiści i specjaliści IT mogą wdrażać aplikacje i wymagane przez nie komponenty w sposób gwarantujący stałą aktualność aplikacji
4. Umożliwiać dokonywanie aktualizacji i poprawek systemu przez Internet
5. Umożliwiać pobieranie darmowych aktualizacji w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bezpłatnie) – wymagane podanie nazwy strony www
6. Posiadać graficzny interfejs użytkownika
7. Umożliwiać debugowanie i diagnozowanie aplikacji, a w szczególności:
    a. Zbieranie danych diagnostycznych dla mechanizmu historycznego debuggowania na serwerach produkcyjnych bez konieczności instalacji zintegrowanego środowiska programistycznego, a poprzez instalację dedykowanego do tego celu agenta,
    b. Zbieranie danych diagnostycznych z określonych zdarzeń w systemie oraz debugowanie błędów historycznych,
    c. Zbieranie wskaźników dotyczących wydajności i zdarzeń zachodzących w aplikacji,
    d. Dostarczać informacji na temat metryk oprogramowania takich jak: współczynnik złożoności, złożoność cyklomatyczna, głębokość drzewa dziedziczenia, linie kodu,

e. Analizę zrzutów pamięci dla aplikacji .NET,
f. Graficzne debugowanie, które umożliwia określania miejsc zatrzymywania wykonywania kodu, analizę wartości zmiennych, definiowanie warunków przerwania działania kodu,
g. Tworzenie kanału komunikacji pomiędzy zintegrowanym środowiskiem programistycznym, a jedną lub wieloma przeglądarkami w celu debuggowania lub wprowadzania zmian w kodzie strony internetowej
h. Statyczna analizę kodu, która umożliwia walidację reguł w zakresie przyjętych wzorców projektowych, analizę potencjalnych problemów wydajnościowych, bezpieczeństwa,
i. Integrację sesji debuggowania z mapą kodu, tworzącą wizualizację drzewa wywołania
j. Debuggowanie aplikacji poprzez interaktywne sesje umożliwiające programiście uruchomić aplikację i analizować wykonywany kod
k. Symulator Windows, który umożliwia uruchomienie wirtualnego komputera z systemem Windows, a dający możliwość wyboru różnych rozdzielczości ekranu, symulowania funkcji dotykowych, symulowania różnych warunków połączenia sieciowego, czy też fizyczną rotację urządzenia
l. Emulator Windows Phone, który umożliwia uruchomienie wirtualnego komputera z systemem Windows, a dający możliwość wyboru różnych rozdzielczości ekranu, symulowania funkcji dotykowych, symulowania różnych warunków połączenia sieciowego, czy też fizyczną rotację urządzenia, generowanie przykładowych zmian w położeniu GPS wirtualnego urządzenia
m. Visual Studio Emulator dla Android, który wspiera różne wersje systemu Android, różne rozmiary ekranu oraz różnego rodzaju urządzenia. Umożliwia symulowanie zmian w sensorach takich jak: akcelerometr, lokalizacja, a także w położeniu GPS, symulacji sieci lub baterii.

2. Umożliwiać testowanie, a w szczególności:
   a. Wykonywać testy obciążeniowe i wydajnościowe stron internetowych wg. zdefiniowanych reguł z możliwością symulacji różnych środowisk takich jak łącze internetowe czy przeglądarka internetowa,
   b. Analizowanie kodu .NET i generowanie danych testowych wraz z testami jednostkowymi,
   c. Izolowanie kodu poprzez podmienianie kawałków kodu za pomocą stub (podmiana klasy na ekwiwalent implementujący ten sam interfejs) lub shim (podmiana wykonywanego kodu na inny kod w sytuacji, kiedy kod nie może zostać podmieniony),
   d. Informować o ilości pokrytego testami kodu w solucji,
   e. Umożliwiać tworzenie z poziomu kodu testów interfejsu graficznego, które będą mogły symulować wykonywanie konkretnych zadań w aplikacji,
   f. Ręczne wykonywanie testów, wraz z możliwością wykonywania krok po kroku, dodawania komentarzy do poszczególnych kroków,
   g. Tworzenie nagrań wykonywania testów wraz z możliwością tworzenia odpowiednich bugów i scenariuszy testowych do dalszego wykonania,
   h. Zarządzanie scenariuszami testowymi dla rozwiązanie,
   i. Przewijanie testów ręcznych do określonego kroku w celu przyspieszenia wykonywania całego testu, a w szczególności jego powtarzalnych, niewymagających interakcji człowieka elementów,

   j. Możliwość rozszerzania wbudowanej funkcjonalności testowania, umożliwiającym wykorzystanie innego silnika testów niż wbudowany domyślnie w zintegrowane środowisko programistyczne,
   k. Tworzenie testów jednostokowych jako wbudowany element w kreatory graficzne zintegrowanego środowiska programistycznego.
3. Posiadać zintegrowane funkcje programistyczne, a w szczególności:
   a. Znajdowanie zmian w kodzie i innych elementów,
   b. Możliwość podejrzenia oraz zmian w kodzie bez otwierania dodatkowego okna,
   c. Wyszukiwanie identycznych lub podobnych fragmentów kodu,
   d. Refaktoryzacja, czyli łatwe zmiany w kodzie aplikacji, takie jak: wyodrębnienie metody, zmiana nazwy, enkapsulacja pola, wyodrębnienie interfejsu, usunięcie parametrów funkcji, zmiana kolejności parametrów funkcji
   e. Umożliwiać wdrażanie rozwiązań internetowych wykorzystujących funkcjonalności One-Click Publish,
   f. Możliwość rozszerzania funkcjonalności zintegrowanego środowiska programistyczne poprzez pisanie własnych wtyczek lub korzystanie z wtyczek dostarczanych w galerii rozszerzeń,
   g. Wsparcie dla wielu wersji frameworka .NET, dzięki czemu najnowsze środowisko programistyczne może być wykorzystywane także do tworzenia, utrzymywania starszych wersji aplikacji,
   h. Posiadać dedykowane narzędzie do projektowania i tworzenia interfejsu graficznego aplikacji – program Blend,
   i. Wsparcie i obsługę języka JavaScript oraz biblioteki jQuery
   j. Kompatybilność solucji i projektów z Visual Studio 2012 SP1 oraz Visual Studio 2012.
4. Wspierać tworzenie aplikacji, działających na różnych platformach i w różnych środowiskach, a w szczególności:
   a. Aplikacje typu Windows Desktop – aplikacje okienkowe,
   b. Aplikacje Windows Phone oraz Windows Store,
   c. Aplikacje Universal Windows Platform,
   d. Aplikacje Internetowe – ASP.NET,
   e. Rozwiązania dla Office 365, Office oraz SharePoint,
   f. Aplikacje Biznesowe dla Office 365,
   g. Aplikacje Biznesowe wykorzystujące technologię LightSwitch,
   h. Rozwiązania Chmurowe, działającego w oparciu o Microsoft Azure,
   i. Rozwiązania dla SQL Server przy wykorzystaniu narzędzi SQL Server Data Tools,
   j. Tworzenie rozwiązań w oparciu o platformę Apache Cordova
   k. Tworzenie rozwiązań wieloplatformowych przy wykorzystaniu języka C++
   l. Aplikacje Python
   m. Aplikacje Node.js
5. Wspierać procesy tworzenia architektury oraz modelowania aplikacji, a w szczególności
   a. Umożliwiać tworzenie diagramów warts architektury aplikacji,
   b. Walidację kodu aplikacji względem zaprojektowanej architektury,
   c. Umożliwiać tworzenie diagramów UML zgodnych z wersją 2.0,
   d. Umożliwiać tworzenie grafów zależności wraz z mapą kodu
6. Umożliwiać tworzenie i zarządzanie środowiskami testowymi przy wykorzystaniu funkcji Lab Management, a w szczególności:
   a. Tworzenie oraz kasowanie wirtualnych środowisk testowych,

   b. Tworzenie środowisk na bazie zdefiniowanych szablonów,
   c. Umożliwiać przechwytywanie stanu całego środowiska
7. Udostępniać poprzez subskrypcję aplikacji na potrzeby rozwoju i testowanie oprogramowania, taki jak: Microsoft Azure, Windows, Windows Server, Windows Embedded, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange, Microsoft Office, Microsoft Dynamics
8. Umożliwiać automatyczną synchronizację ustawień środowiska pomiędzy różnymi stacjami roboczymi
9. Umożliwiać zgłaszanie oraz zarządzanie żądaniami dokonania oceny kodu przez innych członków zespołu

Część nr 12 - SYSTEM OPERACYJNY – 5 SZT.

Zakup systemu operacyjnego w wersji dla serwera 16 Core, zasada licencjonowania w oparciu o rdzenie. Proponowana wersja ma być najnowszą wersją systemu operacyjnego, spełniającą co najmniej następujące cechy:

- Ze względu na posiadaną przez zamawiającego domenę opartą na rozwiązaniu Windows 2016 i polityce kont synchronizowanych z MS Active Directory, system musi umożliwiać bezproblemową współpracę z tymi rozwiązaniami;
- Ze względu na politykę bezpieczeństwa stosowaną u Zamawiającego system musi bezproblemowo pracować w domenie opartej na Windows 2016 oraz w pełni wykorzystywać funkcjonalność domeny Windows;
- Uprawnienia do wirtualizacji : 2 wirtualne maszyny lub 2 kontenery Hyper-V
- Limit pamięci RAM: 24 TB RAM;
- Limit CPU: nieograniczona ilość rdzeni;
- Współpraca z procesorami o architekturze x64;
- Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym;
- Możliwość budowania klastrów składających się z 64 węzłów;
- Możliwość federowania klastrów typu failover w zespół klastrów z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu;

- Możliwość uruchomienia roli klienta i serwera czasu (NTP);
- W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych;

- W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.

- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego
- Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d. umożliwiają zdefiniowanie list kontroli dostępu
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu

o ich zawartość;

- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się

bezpieczeństwem informacji;

- Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET;
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów;
- Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych;
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe;

- Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji;

- Mechanizmy logowania w oparciu o:
    a. login i hasło,
    b. karty z certyfikatami (smartcard),
    c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
- Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
    a. kreślonych grup użytkowników,
    b. zastosowanej klasyfikacji danych,
    c. centralnych polityk dostępu w sieci,
    d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play);
- Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach;
- Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
- Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        - bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. zdalna dystrybucja oprogramowania na stacje robocze.

d. praca zdalna na serwerze z wykorzystaniem terminala lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
    - Dystrybucję certyfikatów poprzez http,
    - Konsolidację CA dla wielu lasów domeny,
    - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f. szyfrowanie plików i folderów.
g. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec)
h. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi
i. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
j. serwis udostępniania stron WWW
k. wsparcie dla protokołu IP w wersji 6 (IPv6).
l. wsparcie dla algorytmów Suite B (RFC 4869).
m. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na posiadanych komputerach z systemem Windows.
n. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
o. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (Hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
p. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu fail-over z jednoczesnym zachowaniem pozostałej funkcjonalności.
q. mechanizmy wirtualizacji mające wsparcie dla:
    - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
    - obsługi ramek typu jumbo frames dla maszyn wirtualnych.
    - obsługi 4-KB sektorów dysków,
    - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
    - możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
    - możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej
    - możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
r. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
s. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
t. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek.
u. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

v. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

- Graficzny interfejs użytkownika;
- Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu;
- Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa;
- Oparta na przeglądarce aplikacja do zarządzania serwerami, klastrami, hiperkonwergentną infrastrukturą i posiadanymi komputerami z systemem Windows 10
- W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie

zasobów sprzętowych serwera.

- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.