

Szczegółowy Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest dostawa licencji oprogramowania Microsoft 365 A5 lub równoważnych subskrypcji pakietu usług hostowanych - subskrypcja na użytkownika wraz z świadczeniem usług wsparcia.

Przedmiot zamówienia obejmuje:

- 1) dostawę 750 szt. licencji Microsoft 365 A5, lub równoważnych, na okres 36 miesięcy od dnia 1 stycznia 2025 r. (zamówienie gwarantowane);
- 2) dostawę 4 szt. licencji Microsoft Teams Rooms Pro, lub równoważnych, na okres 36 miesięcy od dnia 16 lutego 2025 r.;
- 3) w ramach zamówienia opcjonalnego, w przypadku potrzeby zgłoszonej przez Zamawiającego, dostawę do 50 szt. licencji Microsoft 365 A5 lub równoważnych przez okres 1 miesiąca – do maksymalnie 50 (pięćdziesięciu) sztuk miesięcznie, minimum 10 (dziesięć) subskrypcji miesięcznie (Prawo Opcji);
- 4) świadczenie usługi wsparcia technicznego przez Wykonawcę.

1. Wymagania ogólne

- 1) oprogramowanie musi pochodzić bezpośrednio od Producenta lub z oficjalnych i autoryzowanych przez Producenta kanałów dystrybucyjnych. Zamawiający wymaga, aby Wykonawca posiadał kwalifikacje i uprawnienia wymagane do prawidłowej realizacji przedmiotu zamówienia;
- 2) licencje muszą pozwalać na swobodne przenoszenie pomiędzy komputerami (np. w przypadku wymiany sprzętu);
- 3) gwarancja dostępności najnowszej wersji oprogramowania oraz bieżące jego poprawki i uaktualnienia w trakcie trwania umowy;
- 4) możliwość wykorzystania wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego;
- 5) Zamawiający dopuszcza oferowanie produktów o szerszej niż opisana funkcjonalności;
- 6) W ramach procedury odbiorczej Wykonawca w terminie do dnia 1 stycznia 2025 r. zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym ze strony Zamawiającego osobom na:
 - a) pobieranie oprogramowania,
 - b) pobieranie kluczy aktywacyjnych do oprogramowania,
 - c) sprawdzanie liczby zakupionych licencji w wykazie oprogramowania.

2. Usługa wsparcia technicznego

Wykonawca zapewni usługę wsparcia technicznego, konsultacje dla zaproponowanego rozwiązania oraz świadczenie pomocy zdalnej administratorom Zamawiającego, która będzie realizowana przez zespół specjalistów po stronie Wykonawcy posiadających odpowiednie kwalifikacje oraz przez autoryzowaną pomoc techniczną w dni robocze w języku polskim w okresie 36 miesięcy od dnia 1.01.2025 r., w wymiarze nie przekraczającym 300 godz. Usługa obejmuje w szczególności:

- 1) konfigurację i instalację oprogramowania, w szczególności konfigurację kont, ustawienia domen, konfigurację poczty e-mail;
- 2) zapewnienie prawidłowego uruchomienia usług;
- 3) wsparcie migracji danych z innych platform, w tym przenoszenie wiadomości e-mail, kontaktów, kalendarzy i plików;
- 4) wsparcie w zarządzaniu użytkownikami;
- 5) wsparcie w zarządzaniu licencjami;
- 6) konfigurację grup i uprawnień;
- 7) wsparcie przy problemach z logowaniem;
- 8) wsparcie w konfiguracji ustawień bezpieczeństwa, w szczególności:
 - a) uwierzytelnienie wieloskładnikowe (MFA),
 - b) zarządzanie urządzeniami mobilnymi,
 - c) polityki ochrony danych,
 - d) audyt bezpieczeństwa,
 - e) dostosowaniu konfiguracji produktu do specyficznych potrzeb organizacji,
 - f) personalizacji interfejsu;
 - g) automatyzacji procesów biznesowych;
 - h) integracji z innymi aplikacjami biznesowymi.

Kategorie zgłoszeń:

- 1) Krytyczny błąd - wada uniemożliwiająca użytkownikom korzystanie z usługi lub jej fragmentu oraz naruszenie bezpieczeństwa usługi (dostęp do danych lub funkcji usługi z pominięciem mechanizmów zabezpieczeń);
- 2) Poważny błąd - nieprawidłowość działania usługi, która wpływa w istotny sposób na wyniki pracy, ogranicza funkcjonalność usługi, w wyniku czego praca jest utrudniona, ale możliwa;
- 3) Usterka - dysfunkcje, czy uciążliwości utrudniające działanie usługi.

Wykonawca zobowiązany jest podjąć niezwłocznie po przyjęciu zgłoszenia czynności zmierzające do jego zdiagnozowania oraz podjęcia naprawy, jednak nie później niż w terminach wskazanych poniżej.

O rozpoczęciu diagnozy, wyniku diagnozy oraz podjęciu czynności zmierzających do naprawy błędu lub usterki Wykonawca powiadomi Zamawiającego drogą elektroniczną.

Kategoria zgłoszenia	Maksymalny czas reakcji (w trybie 24/7/365)	Maksymalny czas naprawy (w trybie 24/7/365)
Krytyczny błąd	15 min.	2 godz.
Poważny błąd	1 godz.	4 godz.
Usterka	4 godz.	16 godz.

Czas reakcji – czas podjęcia działań w celu przeprowadzenia diagnostyki i lokalizacji usterki lub błędu.

Czas naprawy – czas liczony od chwili potwierdzenia wystąpienia błędu lub usterki do chwili ich usunięcia.

3. Wymagania dla oprogramowania równoważnego

Opis kryteriów równoważności dla oprogramowania Microsoft 365 A5 oraz Microsoft Teams Rooms Pro stanowi

Załącznik nr 1 do SOPZ.

Opis wymagań dla oprogramowania równoważnego**1. Wymagania ogólne:**

- 1) dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy,
- 2) 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,
- 3) możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
- 4) dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
- 5) możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej,
- 6) możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory,
- 7) 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”,
- 8) możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
- 9) wbudowane w platformę mechanizmy zabezpieczające przed atakami DDoS,
- 10) przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km,
- 11) możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego,
- 12) zobowiązania umowne potwierdzające zgodność z rozporządzeniem RODO i potwierdzające rolę Dostawcy usługi jako przetwarzającego dane,
- 13) zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
- 14) gwarancję usunięcia danych Zamawiającego z Platformy po zakończeniu umowy,
- 15) 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;
- 16) Zamawiający dopuszcza oferowanie Produktów o szerszej niż opisana funkcjonalności,
- 17) z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga oferty zawierającej Produkty, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania,

monitorowania i wsparcia technicznego oraz jednolitych mechanizmów wykorzystania tożsamości cyfrowej,

- 18) Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym;
- 19) 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.

2. Wymagania dotyczące usługi hostowanej:

Pakiet subskrypcji powszechnie dostępnej, standardowej usługi hostowanej (on-line) typu COTS (Commercial Of-The-Shelf) ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line – usługi zarządzania tożsamością użytkowników, portalu wewnętrznego, poczty elektronicznej, narzędzi wiadomości błyskawicznych, konferencji głosowych i video, repozytorium dokumentów, usług bezpieczeństwa, usług analizy danych, wewnętrznego serwisu społecznościowego oraz edycji dokumentów biurowych on-line (dalej Usługi). Ponadto musi zawierać subskrypcję pakietu biurowego.

- 1) 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,
- 2) wbudowana usługa zarządzania tożsamością użytkowników musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory,
- 3) możliwość dodawania do 900 własnych nazw domenowych,
- 4) dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup,
- 5) wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików,
- 6) ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day,
- 7) gwarantowana dostępność usług platformy na poziomie 99,9%,
- 8) zastosowanie w Platformie powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy, w szczególności:
 - a) ISO 27001, ISO 27002, ISO 27017, ISO 27018
 - b) UK G-Cloud
 - c) SOC 1, SOC 2
 - d) Open Authentication Standard – OAuth
- 9) dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy.

- 10) 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,
- 11) dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składanych w usłudze danych Zamawiającego,
- 12) możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
- 13) dostępność mechanizmu uwierzytelnienia wieloskładnikowego,
- 14) 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”.
- 15) dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
- 16) wbudowane w platformę mechanizmy zabezpieczające przed atakami DDoS,
- 17) przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km,
- 18) w okresie obowiązywania subskrypcji Usługa będzie przechowywać dane i umożliwiać uprawnione przetwarzanie danych, które pozostają wyłączną własnością Zamawiającego. Po zakończeniu okresu subskrypcji, 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,
- 19) dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS,
- 20) subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich,
- 21) subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego,
- 22) centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego,
- 23) Usługa musi odpowiadać wymaganiom prawa Europejskiego w zakresie ochrony danych osobowych w tym realizować zapisy Decyzji Komisji Europejskiej z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych,
- 24) Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
- 25) Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji,
- 26) zobowiązania umowne potwierdzające zgodność z rozp. RODO i potwierdzające rolę operatora usługi jako przetwarzającego dane,
- 27) zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składanych w usłudze danych po stronie Zamawiającego,

- 28) mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług,
- 29) gwarancja 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.

3. Wymagania dotyczące usługi poczty elektronicznej on-line:

- 1) Usługa musi umożliwiać:
 - a) obsługę poczty elektronicznej,
 - b) zarządzanie czasem,
 - c) zarządzania zasobami,
 - d) zarządzanie kontaktami i komunikacją;
- 2) Usługa musi dostarczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:
 - a) zarządzania użytkownikami poczty,
 - b) wsparcia migracji z innych systemów poczty,
 - c) wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
 - d) wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowaną poczty;
- 3) dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:
 - a) oprogramowania Outlook (2016 i 2019),
 - b) przeglądarki (Web Access),
 - c) urządzeń mobilnych;
- 4) wymagane cechy usługi to:
 - a) skrzynki pocztowe dla każdego użytkownika o pojemności minimum 100 GB,
 - b) standardowy i łatwy sposób obsługi poczty elektronicznej,
 - c) obsługa najnowszych funkcji Outlook 2013 i 2016, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Edge, Google Chrome, Firefox i Safari,
 - d) 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,
 - e) bezpieczny dostęp z każdego miejsca, w którym jest dostępny Internet;
- 5) usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:
 - a) funkcjonalność podstawowa:
 - odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych,
 - mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata,
 - tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami,

- 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,
 - wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości;
- b) funkcjonalność wspierająca pracę grupową:
- możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości,
 - udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu,
 - podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze,
 - 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,
 - tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań,
 - obsługa list i grup dystrybucyjnych,
 - dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych,
 - możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwi szybkie i wygodne ustalenie harmonogramu,
 - możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności,
 - widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami,
 - 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,
 - transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego,
 - dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów – z poziomu urządzeń mobilnych,
 - udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail;
- c) funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:

- centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, archiwizacja,
 - definiowanie limitu rozmiaru skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników,
 - możliwość wprowadzenia modelu kontroli dostępu, który umożliwi nadanie specjalistom uprawnień do wykonywania określonych zadań,
 - możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne,
 - możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów,
 - 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,
 - 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.
 - Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
 - Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
 - Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.
- d) wsparcie dla użytkowników mobilnych:
- 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 opisanej w punkcie a). Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem,
 - możliwość „lekkiej” synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
 - możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu Smart Phone,

- 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,
- umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej,
- obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Edge, Google Chrome, Apple Safari i Mozilla Firefox;

4. 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,

Portale on-line muszą posiadać następujące cechy dostępne bezpośrednio jako wbudowane właściwości produktu:

a) interfejs użytkownika:

- 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),

- wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0,
 - praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów,
 - tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego,
 - umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy);
- b) projektowanie stron:
- wbudowane intuicyjne narzędzia projektowania wyglądu stron,
 - wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML,
 - wsparcie dla ASP.NET, Apache, C#, Java i PHP,
 - możliwość osadzania elementów iFrame w polach HTML na stronie;
- c) integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
- wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci wiadomości e-mail,
 - 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,
 - możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do wiadomości e-mail,
 - 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,
 - wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services;
- d) usługa portalu on-line musi mieć wbudowaną funkcjonalność udostępniania użytkownikom komponentów pakietu biurowego on-line dostępnego przez przeglądarkę.

5. Pakiet biurowy on-line musi spełniać następujące wymagania:

- 1) interfejs 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) posiada kompletny i publicznie dostępny opis formatu,

-
- b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766),
- 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 2010 i 2016 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 2010 i 2016, 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,
 - b) prezentowanie przy użyciu projektora multimedialnego,
 - c) drukowanie w formacie umożliwiającym robienie notatek,
 - d) zapisanie jako prezentacja tylko do odczytu,
 - e) nagrywanie narracji i dołączanie jej do prezentacji,
 - f) opatrywanie slajdów notatkami dla prezentera,
 - g) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
 - h) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
 - i) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
 - j) możliwość tworzenia animacji obiektów i całych slajdów,
 - k) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,
 - l) pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.
- 7) narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych musi umożliwiać:
- a) pisanie, zaznaczanie, rysowanie, nagrywanie i odtwarzanie filmów, umieszczanie zdjęć i ich prezentację,
 - b) nadanie poszczególnym notesom statusu prywatnego lub publicznego,
 - c) automatyczne zapisywanie wszystkiego co jest w nim tworzone,
 - d) szybkie i łatwe udostępnianie bez względu z jakiego urządzenia korzysta i gdzie się znajduje,
 - e) pracę grupową tzn. praca w jednym notesie wielu osób jednocześnie.

6. Usługa komunikacji wielokanałowej on-line (UKW) 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:

- a) 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 pulpitych w systemach Windows oraz

- współdzielenie dokumentów z możliwością przejmowania kontroli i edycji przez uprawnionych uczestników,
- b) 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,
 - c) możliwość zapraszania do spotkań zdalnych użytkowników zewnętrznych nieposiadających licencji usługi.
 - d) możliwość oceny jakości komunikacji głosowej i wideo,
 - e) 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,
 - f) dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką UKW lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub specjalizowanych urządzeń stacjonarnych typu telefon IP, kamera dookólna czy duże monitory lub projektory,
 - g) 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,
 - h) 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,
 - i) możliwość stworzenia poczekalni dla dołączających użytkowników z dołączaniem ich decyzją uprawnionych osób,
 - j) możliwość zastąpienia tła lub jego rozmycia w przypadku transmisji video,
 - k) możliwość zakładania przestrzeni dla grup użytkowników z własnym chatem, repozytorium dokumentów i notatkami pozwalającymi na wyseparowaną pracę w ramach zespołów z możliwością udostępniania zawartości przestrzeni wszystkim lub wskazanym użytkownikom,
 - l) możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych,
 - m) możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej),
 - n) możliwość nagrywania telekonferencji przez uczestników,
 - o) zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW,
 - p) możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej,

-
- q) możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
 - r) dostępność aplikacji klienckiej usługi UKW (komunikatora) z funkcjonalnością:
 - listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielenia grup kontaktów typu ulubione lub ostatnie,
 - historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
 - wsparcia telekonferencji, w szczególności 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 pulpitu, możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,
 - integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności,
 - definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z UKW;
- 5) wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji UKW 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 UKW dostępne dla użytkowników posiadających odpowiednie uprawnienia licencyjne i 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 sign-on) dla uprawnionego dostępu do usług UKW,
 - b) dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon),
 - c) współdzielenie mechanizmów UKW z pocztą głosową, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:
 - uruchamiania funkcji komunikacyjnych UKW 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.
- 6) Możliwość sterowania połączeniami telefonicznymi (funkcjonalność centrali PBX w chmurze)
- a) Możliwość korzystania z poczty głosowej,
 - b) Możliwość korzystania z kolejki połączeń,
 - c) Możliwość wykorzystywania funkcjonalności automatycznej asystencji.

7. Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 5 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.

8. Usługi bezpieczeństwa wbudowane w Produkt muszą pozwalać na:

- 1) 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;
- 2) wykrywanie słów kluczowych w przesyłanych wiadomościach i sygnalizowanie potencjalnego wycieku informacji;
- 3) możliwość ograniczania przedziału czasowego uprawnionego dostępu użytkowników do informacji;
- 4) możliwość stosowania wymogu wieloskładnikowego uwierzytelniania.

9. Usługi analizy danych wbudowane w Produkt

- 1) konfigurowanie on-line kokpitów informacyjnych wizualizujących wyniki analiz danych;
- 2) gotowe mechanizmy podłączania różnego rodzaju danych strukturalnych, semi-strukturalnych i niestructuralnych;
- 3) korzystanie z gotowych algorytmów i modeli analizy oraz budowa własnych modeli w języku R.

10. 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 umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,
- 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 pakietach biurowych;
- 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. 2012, poz. 526),
 - c) umożliwia kreowanie plików w formacie XML,
 - d) wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES.
- 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 makropoleczeń, 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 prywatną (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 nagłówek i stopek stron,
- i) śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumentach.
- 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 2010, 2013 i 2016 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) obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,
- f) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
- g) wyszukiwanie i zamianę danych,
- h) wykonywanie analiz danych przy użyciu formatowania warunkowego,
- i) tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS,
- j) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,

- k) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
 - l) formatowanie czasu, daty i wartości finansowych z polskim formatem,
 - m) zapis wielu arkuszy kalkulacyjnych w jednym pliku,
 - n) inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł,
 - o) możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechnaniu znacznikiem myszy na dany rodzaj wykresu),
 - p) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
 - q) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
- 12) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać tworzenie prezentacji, które będą posiadały funkcje:
- a) prezentowanie przy użyciu projektora multimedialnego,
 - b) drukowanie w formacie umożliwiającym robienie notatek,
 - c) zapisanie jako prezentacja tylko do odczytu,
 - d) nagrywanie narracji i dołączanie jej do prezentacji,
 - e) opatrywanie slajdów notatkami dla prezentera,
 - f) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
 - g) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
 - h) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
 - i) możliwość tworzenia animacji obiektów i całych slajdów,
 - j) 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,
 - k) pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, MS PowerPoint 2013 i 2016.
- 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,
 - b) edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych,
 - c) tworzenie bazy danych przy użyciu zdefiniowanych szablonów,
 - d) połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.
 - e) Możliwość pracowania z danymi w oparciu o język SQL
- 15) Narzędzie do zarządzania informacją prywatną (poczta 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 użytkownikom,
- 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 10,
- d) możliwość zintegrowania uwierzytelniania użytkowników z usług 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 UKW:
 - 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 pulpików,
 - 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 UKW, zdjęciami użytkowników, listą dostępnych do komunikacji z nimi kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji oraz wydzielenia 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 UKW,
- 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.

11. Aplikacje wspierające analitykę

- 1) Użytkownicy mają mieć dostęp do samoobsługowej analityki, tak aby umożliwić im wizualizowanie danych przy użyciu pulpitu nawigacyjnego i raportów na żywo, jak również umożliwić udostępnianie ww. szczegółowej informacji w całej organizacji.

Dodatkowo usługa powinna realizować następujące funkcje:

- a) Współpraca i Analityka
 - Dostęp do aplikacji mobilnej
 - Publikowanie raportów na potrzeby udostępniania i współpracy
- b) Przygotowywanie, modelowanie i wizualizacja danych
 - Limit rozmiaru modelu 1GB
 - Częstotliwość odświeżania 8/dzień
 - Połącz się z ponad 100 źródłami danych
 - Tworzenie raportów i wizualizacji za pomocą dedykowanego programu
 - Osadzanie interfejsów API i kontrolek
 - Wizualizacje technologii AI
- c) Ład i administracja
 - Zabezpieczenia i szyfrowanie danych
 - Metryki dotyczące tworzenia, używania i publikowania zawartości
 - Maksymalny rozmiar magazynu 10 GB na użytkownika

- 2) Platforma ma umożliwiać sprawniejszą pracę dzięki analizie osobistej produktywności a w szczególności:

- a. Ułatwi zaplanowanie czasu na pracę w skupieniu

- b. Pomoże w zapanowaniu nad zadaniami i wiadomościami e-mail
- c. Podtrzyma komunikację z ważnymi osobami
- d. Umożliwi tworzenie wzorców pracy
- e. Udostępni chroniony wgląd w swoje dane osobiste i analizę opartą na własnych wzorcach pracy (ochrona prywatności)

12. Aplikacje ochrony przed zagrożeniami

- 1) Zaawansowana ochrona przed zagrożeniami w usłudze poczty elektronicznej.
 - a) Kontroluje poufne dane biznesowe za pomocą wbudowanych zasad ochrony przed utratą danych opartych na standardach zgodnych z przepisami, takich jak dane osobowe (PII, personally identifiable information) i PCI (Payment Card Industry),
 - b) Ułatwia identyfikowanie, monitorowanie i chronienie danych poufnych przez dogłębną analizę zawartości
- 2) Analiza zagrożeń usługi Office
 - a) Usługa udostępnia szeroki wgląd w środowisko zagrożeń, ułatwiając wyciąganie praktycznych wniosków,
 - b) Zapewnia pro-aktywne cyberbezpieczeństwo, co wspomaga obniżanie kosztów
- 3) Zaawansowane zabezpieczenia Office
 - a) Ochrona użytkowników przed wyrafinowanymi zagrożeniami ukrytymi w wiadomościach e-mail, załącznikach i linkach. Dzięki skrytce klienta można ograniczyć dostęp do danych tylko do wstępnie wyznaczonych, zatwierdzonych przez administratora osób uwierzytelnianych dwuskładnikowo, zyskując większą kontrolę i przejrzystość.
 - b) Umożliwiają lepszy wgląd w środowisko usługi Office i kontrolę nad nim
- 4) Rozwiązanie do zbierania elektronicznych materiałów dowodowych
 - a) Zapewnia kompleksowy przepływ pracy umożliwiający przechowywanie, gromadzenie, przeglądanie, analizowanie i eksportowanie treści, które odpowiadają wewnętrznym i zewnętrznym dochodzeniom Twojej organizacji.
 - b) Pozwala również zespołom prawnym zarządzać opiekunami i całym przepływem powiadomień o wstrzymaniu prawnym w celu komunikowania się z opiekunami zaangażowanymi w sprawę.
 - c) Usługa pozwalająca na utworzenie sprawy zaawansowanego zbierania elektronicznych materiałów dowodowych,
 - d) Usługa pozwalająca na przepływ pracy zaawansowanego zbierania elektronicznych materiałów dowodowych.
 - e) Umożliwienie dodawania opiekunów do sprawy, zarządzania opiekunami w sprawie i przeglądania działań opiekuna, przeszukując dziennik inspekcji,
 - f) Blokada prawna, obejmuje tworzenie i automatyzację przepływu pracy powiadomień oraz sposobu, w jaki użytkownik potwierdził powiadomienie o wstrzymaniu.

- g) Indeksowanie zaawansowane, sposoby naprawiania błędów indeksowania w zawartości z lokalizacji przechowujących i niepobieralnych zawartości, a następnie przysłać skorygowane pliki do zbioru recenzji lub korygować poszczególne błędy przetwarzania w zestawie do recenzji.
- h) Dowiedz się, jak wyszukiwać treści w zabezpieczonych lokalizacjach zawartości, a następnie dodawać odpowiednie dane sprawy do zbioru recenzji.
- i) Zbieranie danych do sprawy
- j) Zarządzanie zestawami recenzji, poprzez przeglądanie, tworzenie zapytań, filtrowanie i oznaczanie dokumentów w zestawie do recenzji.
- k) Analizuj dane w zestawie recenzji, poprzez analizę dokumentów w zestawie do recenzji. Wyniki przeprowadzonej analizy obejmują wykrywanie prawie duplikatów, tworzenie wątków w wiadomościach e-mail i identyfikację motywów.
- l) Eksportowanie danych ze sprawy do zewnętrznej oceny.

13. Usługa zarządzania tożsamością

- 1) Usługa filtrowania poczty e-mail, która pomaga chronić organizację przed zaawansowanymi zagrożeniami dla poczty e-mail i narzędzi do współpracy, takimi jak wyłudzenie informacji, włamanie do firmowej poczty e-mail i ataki złośliwego oprogramowania. Ochrona usługi zapewni również funkcje badania, wyszukiwania zagrożeń i korygowania, aby pomóc zespołom ds. zabezpieczeń w efektywnym identyfikowaniu, określaniu priorytetów, badaniu zagrożeń i reagowaniu na nie.
 - a) Funkcja bezpiecznych załączników zapewniają dodatkową warstwę ochrony załączników wiadomości e-mail. W szczególności bezpieczne załączniki używają środowiska wirtualnego do sprawdzania załączników w wiadomościach e-mail przed ich dostarczeniem do adresatów (proces znany jako detonacja).
 - b) Funkcja skanowania bezpiecznych linków chroni organizację przed złośliwymi linkami używanymi podczas wyłudzenia informacji i innych ataków.
 - c) Możliwość konfigurowania ustawień ochrony przed wyłudzeniem informacji są dostępne w organizacjach platformy z skrzynkami pocztowymi, autonomicznymi organizacjami skrzynek pocztowych.
 - d) Portal do uruchamiania realistycznych scenariuszy ataków w organizacji. Te symulowane ataki mogą pomóc w zidentyfikowaniu i znalezieniu narażonych użytkowników, zanim rzeczywisty atak wpłynie na wyniki finansowe.
 - e) Funkcja obejmuje zautomatyzowane procesy badania w odpowiedzi na znane zagrożenia, które istnieją obecnie. Odpowiednie akcje korygowania oczekują na zatwierdzenie, umożliwiając zespołowi ds. operacji zabezpieczeń reagowanie na wykryte zagrożenia.
 - f) Narzędzie do raportowania niemal w czasie rzeczywistym, które pomaga zespołom operacji zabezpieczeń (SecOps) badać zagrożenia i reagować na nie.
- 2) Zaawansowany system operacyjny, który umożliwia zarządzanie, bezpieczeństwo i wsparcie dla zaawansowanych funkcji typu:

- a) Funkcja zabezpieczeń systemu Windows typu BitLocker, która zapewnia szyfrowanie całych woluminów, eliminując zagrożenia związane z kradzieżą danych lub ujawnieniem ich z utraconych, skradzionych lub niewłaściwie zlikwidowanych urządzeń.
 - b) Funkcja pozwalająca utrzymać bezpieczeństwo sieci, ograniczając połączenia według typów ruchu, aplikacji i metod uwierzytelnienia.
 - c) Funkcja pomagająca kontrolować, aplikacje i pliki użytkownicy mogą uruchamiać. Należą do nich pliki wykonywalne, skrypty, pliki Instalatora Windows, biblioteki dołączane dynamicznie (DLL), spakowane aplikacje i spakowane instalatory aplikacji.
 - d) Funkcja do zapobiegania atakom kradzieży poświadczeń, chroniąc skróty haseł NTLM, bilety przyznawania biletów protokołu Kerberos (TGT) oraz poświadczenia przechowywane przez aplikacje jako poświadczenia domeny.
 - e) Funkcja ochrony przed złośliwym oprogramowaniem.
 - f) Ochrona punktu końcowego do zabezpieczeń punktu końcowego przedsiębiorstwa, która pomaga sieciom przedsiębiorstw w zapobieganiu zaawansowanym zagrożeniom, wykrywaniu i badaniu ich oraz reagowaniu na nie.
 - g) Funkcja MDM: zarządzania urządzeniami przenośnymi, które działają podobnie jak punkt odniesienia zabezpieczeń zasad. Ten punkt odniesienia można łatwo zintegrować z dowolnym rozwiązaniem MDM, aby zaspokoić potrzeby operacyjne specjalistów IT, rozwiązując problemy związane z bezpieczeństwem nowoczesnych urządzeń zarządzanych w chmurze.
- 3) Zestaw narzędzi do zarządzania urządzeniami mobilnymi, ochrony przed zagrożeniami, zabezpieczania tożsamości i dostępu, takie jak:
- a) Zintegrowane rozwiązanie do obsługi tożsamości w chmurze i dostępu, zarządzania katalogami, umożliwiania dostępu do aplikacji i ochrony tożsamości, zarządzanie tożsamościami uprzywilejowanymi oraz samoobsługowe zarządzanie dostępem dla użytkowników końcowych.
 - b) Usługa Information Protection do pomagania wykrywaniu, klasyfikowania, ochrony i zarządzania poufnymi informacjami w dowolnym miejscu lub podróży.
 - c) MFA: Uwierzytelnienie wieloskładnikowe
 - d) Mechanizm, który łączy różne sygnały, takie jak użytkownik, urządzenie i lokalizacja, aby automatycznie podejmować decyzje i wymuszać zasady dostępu w organizacji. Obejmuje to uwzględnianie poziomu ryzyka. Dzięki dostępowi warunkowemu można zrównoważyć bezpieczeństwo z produktywnością, stosując odpowiednie mechanizmy kontroli dostępu. Przykłady zasad dostępu warunkowego to instrukcje typu "if-then", np. jeśli użytkownik chce uzyskać dostęp do zasobów, musi wykonać określoną akcję, taką jak uwierzytelnianie wieloskładnikowe.
 - e) Usługa umożliwia użytkownikom zmianę lub resetowanie hasła bez udziału administratora lub pomocy technicznej. Jeśli konto użytkownika jest zablokowane lub zapomni hasło, może postępować zgodnie z monitami, aby odblokować się i wrócić do pracy

- f) Niestandardowe kontrolki współpracujące z ograniczonym zestawem zatwierdzonych dostawców uwierzytelniania. Aby utworzyć kontrolkę niestandardową, należy najpierw skontaktować się z dostawcą, którego chcesz użyć.
- g) SaaS: Bezproblemowe logowanie jednokrotne zapewnia automatyczne logowanie użytkowników, gdy ich urządzenia firmowe połączone z siecią firmową. Gdy ta funkcja jest włączona, użytkownicy nie muszą wpisywać haseł, aby zalogować się do usługi, a zwykle nie muszą nawet wpisywać swoich nazw użytkownika. Ta funkcja zapewnia użytkownikom łatwy dostęp do aplikacji w chmurze bez konieczności używania dodatkowych składników lokalnych.
- h) Usługa typu AIP: Usługa pomaga wykrywać, klasyfikować, chronić i zarządzać poufnymi informacjami w dowolnym miejscu lub podróży.
- i) Usługa typu DLP: Ochrona przed utratą danych to rozwiązanie z dziedziny zabezpieczeń, które identyfikuje przypadki niebezpiecznego lub niewłaściwego udostępniania, przenoszenia lub używania poufnych danych i pomaga zapobiec ich występowaniu. Pomaga ono organizacji w monitorowaniu i ochronie poufnych informacji w systemach lokalnych, w lokalizacjach chmurowych oraz na urządzeniach punktów końcowych. Pomaga również zapewnić zgodność z przepisami, na przykład z Ustawą o przenoszeniu i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA) i Ogólnym rozporządzeniem o ochronie danych (RODO).
- j) Oparte na chmurze rozwiązanie do zarządzania punktami końcowymi. Zarządza ono dostępem użytkowników do zasobów organizacji oraz upraszcza zarządzanie aplikacjami i urządzeniami na wielu urządzeniach, a w tym na urządzeniach przenośnych, komputerach stacjonarnych i wirtualnych punktach końcowych. Dostęp i dane można chronić na urządzeniach osobistych należących do organizacji i użytkowników. Ponadto usługa Intune ma funkcje zgodności i raportowania, które obsługują model zabezpieczeń Zero Trust.
- k) Usługa oparta na chmurze pomagająca chronić pliki i wiadomości e-mail na wielu urządzeniach, w tym telefony i komputery przy użyciu zasad szyfrowania.

14. Aplikacja wspierająca elektroniczny obieg dokumentów

Pakiet Office musi umożliwiać szybką aktualizację i tworzenie dokumentów bezpośrednio w systemie elektronicznej obsługi dokumentów EZD PUW z wykorzystaniem dodatku do systemu Windows AddIn.

15. Usługa komunikacji wielokanałowej on-line wspomagająca wewnętrzną i zewnętrzną komunikację w salach konferencyjnych.

- 1) Wysokiej jakości wideo HD i audio
- 2) Zgodność z urządzeniami PolyStudio 70 oraz PolyTC8
- 3) Integracja z usługą poczty elektronicznej, kalendarzem i usługą komunikacji wielokanałowej on-line;
- 4) Łatwe planowanie i dołączenie do spotkań bezpośrednio z kalendarza;
- 5) Możliwość udostępniania ekranu i współdzielenia plików;
- 6) Interaktywne tablice używane przez uczestników spotkań do rysowania, pisania i dodawania notatek

- 7) Szyfrowanie end-to-end;
- 8) Automatyczne aktualizacje oprogramowania;
- 9) Zgodność z regulacjami takimi jak GDPR i HIPAA;
- 10) Redukcja szumów tła;
- 11) Transkrypcje spotkań na żywo;
- 12) Tłumaczenie na żywo w wielu językach;
- 13) Wsparcie dla szerokiej gamy sprzętu konferencyjnego, w tym kamer, mikrofonów i głośników od różnych producentów;
- 14) Dostosowanie ustawień i konfiguracji według potrzeb organizacji, w tym personalizacja interfejsu użytkownika;
- 15) Narzędzia do analizy spotkań, takie jak statystyki uczestnictwa, czas trwania, wykorzystanie zasobów spotkań;
- 16) Raporty pomagające w optymalizacji wykorzystywania sal konferencyjnych oraz ich zasobów.

16. Wymagania dodatkowe

W przypadku zaproponowania rozwiązania równoważnego, zgodnego z wymienionymi kryteriami równoważności, Wykonawca zobowiązuje się:

- 1) zapewnić warunki i zakres usługi wsparcia producenta dla produktów równoważnych nie gorsze niż usługa określona dla licencji i subskrypcji oferowanych przez firmę Microsoft;
- 2) zapewnić warunki licencji w każdym aspekcie licencjonowania nie gorsze niż dla licencji subskrypcji będących w ofercie firmy Microsoft;
- 3) dostarczone produkty muszą zapewnić pełną kompatybilność z aktualnie funkcjonującym u Zamawiającego oprogramowaniem firmy Microsoft;
- 4) zapewnić, że Produkty równoważne są kompatybilne i w sposób niezakłócony współdziałać będą ze sprzętem i oprogramowaniem systemowym, aplikacyjnym i użytkowym, eksploatowanym u Zamawiającego;
- 5) przywrócić sprawne działanie infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokonać niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po odinstalowaniu Produktów równoważnych w przypadku, gdy zaoferowane Produkty równoważne nie będą właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowodują zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego Zamawiającego.

17. Usługa wdrożenia i migracji

Wykonawca zobowiązuje się do przedstawienia do akceptacji projektu technicznego wdrożenia i migracji, którego celem jest analiza przedwdrożeniowa oraz opis procesu migracji.

Na architekturę systemu Zamawiającego składa się: 1x Exchange Server 2016 CU23 on premise wraz z zainstalowanymi poprawkami przeciw Zero-Day, Active Directory on premise + Azure AD Connector, Office

365 E5, Exchange Online, Sharepoint, MS Teams, OneDrive Online, MS Teams Rooms Pro, Power BI. Wykonawca zrealizuje usługę migracji zasobów Zamawiającego posadowionych na serwerach Microsoft Exchange Server (wolumen danych 250 GB) oraz Microsoft SharePoint ONLINE (wolumen danych 953 witryn, 2,5 TB), w szczególności:

1) Microsoft Exchange Online:

- a) Migracji podlegać będą następujące zasoby:
 - skrzynki pocztowe wraz z wiadomościami i folderami,
 - skrzynki współdzielone,
 - grupy dyskusyjne,
 - zasoby,
 - kontakty,
 - wpisy z kalendarza,
 - zadania.
- b) reguły poczty (przekierowania itp.) Migracja skrzynek pocztowych ma się odbywać w sposób gwarantujący, że żadna wiadomość nie zostanie w tym czasie utracona, przeniesienie skrzynek do chmury nie powoduje jakichkolwiek zmian w dotychczasowych adresach poczty elektronicznej,
- c) Do skrzynki pocztowej przeniesione zostaną wszystkie dane ze skrzynki lokalnej z wyłączeniem wiadomości znajdujących się w folderze Wiadomości-śmieci,
- d) Przeniesione skrzynki do chmury mają być objęte ochroną antyspamową, a zwłaszcza ochroną przed phishingiem (wyłudzeniami),
- e) W usłudze mają zostać uruchomione mechanizmy odzyskiwania poczty:
 - Odtwarzanie całego systemu (disaster recovery). W przypadku awarii całego systemu, operator chmury gwarantuje jego odtworzenie z kopii nie starszej niż 14 dni,
 - Odzyskiwanie usuniętej zawartości (dot. pojedynczych skrzynek). Skrzynki pocztowe mają być wyposażone w dwa poziomy koszy przechowujących usunięte wiadomości.
- f) W trakcie migracji musi zostać uruchomiona usługa informująca o stanie migracji jak również po przeprowadzonej migracji Zamawiający otrzyma Raport Stanu Migracji,
- g) Jeśli usługa migracji będzie realizowana w godzinach pracy, nie może wpływać na dostępność dotychczas wykorzystywanej usługi e-mail Zamawiającego,
- h) Dane skrzynek pocztowych w trakcie migracji będą podlegać szyfrowaniu (musi zostać zagwarantowane bezpieczeństwo danych),
- i) Zamawiający rekomenduje przeprowadzenie migracji tzw. jednorazowej tzn. migracja całego środowiska ma się odbyć w tym samym czasie i dotyczy nie więcej niż 1500 skrzynek,
- j) Wykonawca przed przystąpieniem do migracji przedstawi szczegółową koncepcję migracji uwzględniającą ww. punkty jak również opisze zagrożenia i przedłoży harmonogram prac,
- k) Ww. prace będą prowadzone z udziałem przedstawicieli Zamawiającego.

System po migracji będzie obsługiwał około 950 skrzynek, 450 grup, 30 zasobów, 400 skrzynek współdzielonych, 10 reguł oraz 10 domen. Zamawiający przewiduje dalszy, powolny, wzrost.

- 2) Zamawiającego aktualnie posiada rozwiązanie Microsoft SharePoint online (usługa łączna z usługą OneDrive zajmuje ok. 10 TB).
 - a) Migracji podlegać będzie cała zawartość ww. usługi, w szczególności:
 - Zbiory witryn, witryny,
 - Biblioteki, listy, strony w tym foldery i dokumenty,
 - Użytkownicy i uprawnienia (uprawnienia osób, grup i witryn),
 - Wygląd i działanie (tytuły, linki, logotypy, itp.),
 - Prace zespołów (kalendarze, zadania, notesy, itp.),
 - Lokalne zasoby użytkowników przechowywane w usłudze OneDrive.
 - b) Migracja ma się odbywać w sposób gwarantujący, że żadne dane nie zostaną w tym czasie utracone,
 - c) W przypadku konieczności dokonywania transferów danych musimy zachować ich bezpieczeństwo (szyfrowanie danych lub korzystanie z bezpiecznych kanałów szyfrowania TLS),
 - d) Po przeprowadzonej migracji Zamawiający otrzyma Raport Stanu Migracji (jeśli pojawią się błędy Raport ma również je zawierać),
 - e) Jeśli usługa migracji będzie realizowana w godzinach pracy, nie może wpływać na dostępność dotychczas wykorzystywanej usługi SharePoint, OneDrive Zamawiającego,
 - f) Wykonawca przed przystąpieniem do migracji przedstawi szczegółową koncepcję migracji uwzględniającą ww. punkty jak również opisz zagrożenia i przedłoży harmonogram prac,
 - g) Ww. prace będą prowadzone z udziałem przedstawicieli Zamawiającego.
- 3) Wykonawca zapewni wdrożenie zaproponowanego rozwiązania w następującym zakresie:
 - a) wdrożenie usług rozwiązania równoważnego,
 - b) wdrożenie usługi bezpieczeństwa informacji, która ma pozwala na stworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania. Zamawiający informuje, iż Zamawiającemu zależy aby w oprogramowaniu SIEM - Splunk ES były widoczne lub odczytywalne informacje/logi z oferowanego produktu. Możliwość przekierowania w bezpieczny sposób logów do SIEM - Splunk ES lub inny sposób pozwalający na odczytanie logów generowanych, np. poprzez bezpieczne API i aplikacje/addon w SIEM - Splunk ES. Dobór rozwiązania pozostawiamy Wykonawcy jednakże Zamawiający preferuje wykorzystanie bezpiecznego API.
 - c) ATP (Advanced Threat Protection) wdrożenie usługi skanowania załączników wiadomości e-mail, dokumentów przechowywanych w aplikacjach Zamawiającego w celu lokalizowania i usuwania złośliwej zawartości. Ponadto ATP ma umożliwiać skanowanie adresów URL w wiadomościach e-mail, aby upewnić się, że są one bezpieczne.

Zamawiający wymaga przeniesienia funkcjonalności posiadanych dotychczas oraz konfigurację usług pozwalającą w pełni korzystać z usług przez wszystkich pracowników Zamawiającego.

Usługa wdrożenia i migracji będą realizowane przez zespół specjalistów po stronie Wykonawcy posiadających odpowiednie kwalifikacje oraz przez autoryzowaną pomoc techniczną w dni robocze w języku polskim.

18. Usługa szkoleniowa

Wykonawca zapewni przeprowadzenie certyfikowanych szkoleń dla administratorów Zamawiającego zakończonych otrzymaniem certyfikatu uczestnictwa i certyfikowanym przez producenta.

Szkolenia zostaną przeprowadzone w terminie zgodnym z harmonogramem realizacji zamówienia w terminie ustalonym z Zamawiającym.

19. Usługa integracji

Wykonawca zobowiązuje się do wykonania integracji zaproponowanego rozwiązania z posiadanym przez Zamawiającego systemami:

- 1) SIEM - Splunk ES. Zamawiający posiada licencje Splunk Enterprise i Splunk Enterprise Security aktywne do dnia 24 grudnia 2025 r. (licencja 100GB/dzień). Na potrzeby logów dla zakładanej liczby skrzynek zostanie zarezerwowany limit 15 GB dziennie z obecnie posiadanej licencji. Jeśli integracja wymaga zakupu dodatkowych licencji do SIEM Wykonawca zobowiązany jest do ich zapewnienia;
- 2) FortiMail Virtual Appliance pełniący rolę SMTP Gateway (posiadany przez Zamawiającego FortiMail VM pracuje w trybie Gateway (bramki pocztowej). Zamawiający informuje, iż posiada licencje Gateway Premium wraz z Office 365 API. Jeśli integracja wymaga zakupu dodatkowych licencji lub funkcjonalności Wykonawca zobowiązany jest do ich zapewnienia. Posiadana przez Zamawiającego licencja FortiMail obejmuje 1001 użytkowników. Licencja FortiMail VM jest aktywna do 16 sierpnia 2026 r. Zamawiający wymaga, aby wiadomości pocztowe wchodzące do i wychodzące z platformy były sprawdzane pod kątem wirusów i spamu przez posiadany przez Zamawiającego FortiMail.

Zdarzenia muszą być zbierane ze wszystkich możliwych aplikacji, które oferują tzw. audit logi, w szczególności zdarzenia dotyczące aktywności użytkowników i administratorów.

Zamawiający wymaga wdrożenia / uruchomienia wszelkich usług jeśli usługa ta są wymagane do zawartej w SOPZ integracji z posiadanym przez Zamawiającego oprogramowaniem (Splunk oraz FortiMail).