Opis Przedmiotu Zamówienia

do

planowanego postępowania publicznego

w trybie przetargu nieograniczonego z prawem opcji

na

Dostawę oprogramowania, praw do aktualizacji oprogramowania standardowego oraz dostawę pakietów subskrypcji usług standardowych.

Spis treści

1. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostawa oprogramowania, praw do aktualizacji oprogramowania standardowego, dostawa pakietów subskrypcji usług standardowych (Produktów) w ramach umowy trwającej do 31 grudnia 2025 (dalej nazywanej Umową).
2. Zamawiający zastrzega sobie prawo do rozszerzenia zakresu umowy określonego listą Produktów gwarantowanych w trakcie jej trwania poprzez możliwość udzielania zamówień opcjonalnych w tym samym zakresie asortymentu - zgodnie z zapisami projektu umowy.
3. Zamawiający nie gwarantuje zakupu Produktów opcjonalnych. Zamówienia dotyczące Produktów opcjonalnych będą udzielane w miarę potrzeb Zamawiającego i dostępności budżetu.
4. W opisie przedmiotu zamówienia (tab. 1) Zamawiający przedstawia specyfikację ilościową dotyczącą zakupu Produktów gwarantowanych, których dostawa następuje po podpisaniu umowy zgodnie z jej warunkami.
5. Ceny jednostkowe subskrypcyjnych Produktów opcjonalnych w EUR muszą być tożsame z cenami jednostkowymi odpowiednich Produktów gwarantowanych zawartymi w ofercie Wykonawcy.
6. Zamawiający dopuszcza dostawy Produktów równoważnych do wymienionych w SWZ. Warunki równoważności opisane są w punkcie 1.3 opisu przedmiotu zamówienia.
7. W przypadku oferowania produktów równoważnych lub oferowania ich w równoważnych do opisanych w SWZ programach licencyjnych Wykonawca poniesie całkowity koszt związany z migracją systemów i procesów organizacyjnych obecnie działających u Zamawiającego. Prace takie muszą zostać wykonane w okresie 5-ciu dni roboczych od dnia podpisania umowy.

1.1. Specyfikacja ilościowa

Tab. 1 - Specyfikacja ilościowa przedmiotu zamówienia - Produkty gwarantowane:

L.p.	Numer katalogowy	Nazwa produktu	Liczba produktów gwarantowanych
1	AAD-33168	M365 E5 Unified Sub Per User	5 100
2	7LS-00002	Project Plan3 Shared All Lng Subs VL MV L Per User	10
3	N9U-00002	VisioPlan2 ShrdSvr ALNG SubsVL MVL PerUsr	10
4	JFX-00003	M365 F3 FUSL Sub Per User	1 700
5	9GS-00135	CIS Suite Datacenter Core ALng SA 2L	112
6	9GA-00313	CIS Suite Standard Core ALng SA 2L	632

7	7NQ-00292	SQLSvrStdCore ALNG SA MVL 2Lic CoreLic	24
8		Azure Prepayment	1440*

*Azure Prepayment 1440 jednostek na 3 lata = 480 rocznie = 40 miesięcznie

1.2. Stan obecny

1. Zamawiający eksploatuje aktualnie systemy, oprogramowanie i inne zasoby, związane z niniejszym zamówieniem, zgodnie z zestawieniem poniżej:
    a. System operacyjny komputerów użytkowników – MS Windows 10, 11 Enterprise.
    b. Środowisko serwerowe oparte jest o systemy MS Windows Serwer 2019 działające w klastrze Hyper-V oraz w chmurze MS Azure.
    c. Środowisko Active Directory.
    d. Systemy dziedzinowe wykorzystują bazę danych MS SQL Server.
    e. Poczta elektroniczna opiera się na rozwiązaniu hybrydowym MS Exchange- Microsoft 365.
    f. Zasoby chmury Microsoft 365 na poziomie E3 Enterprise Agreement.
    g. Microsoft 365 dla przedsiębiorstw.
    h. Oprogramowanie zabezpieczenie, typu antywirus: Windows Defender i komputery zabezpieczone również rozwiązaniem ESET.
    i. Intranet oparty o rozwiązanie SharePoint Online.
    j. MDM dla urządzeń mobilnych zarządzany w systemie Microsoft Intune.
    k. Platforma komunikacyjna Microsoft Teams.
    l. Zamawiający eksploatuje również inne zasoby chmury MS Azure, w tym:

Typ	Ilość
Application gateway	2
Application group	1
Application Insights	1
Availability set	3
Connection	1
Container registry	4
Disk	43
Host pool	2
Local network gateway	1
Log Analytics workspace	3
Network interface	34

Network security group	14
Network Watcher	2
Public IP address	5
Recovery Services vault	1
Shared dashboard	1
Snapshot	43
Solution	5
SQL virtual machine	2
SSH key	1
Storage account	8
Virtual machine	32
Virtual network	3
Virtual network gateway	1
Workspace	2

1.3. Minimalne wymagania ogólne w zakresie dostaw

1. Oferowane przez Wykonawcę Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).
2. Zamawiający dopuszcza oferowanie Produktów o szerszej niż opisana funkcjonalności oraz Produktów następczych zastępujących zaoferowane, spełniających wymagania SWZ.
3. Zamawiający wymaga dostawy Produktów na warunkach przewidzianych przez producenta Produktów lub jego spółek zależnych (Dostawcy).
4. Zamawiający wymaga dostawy Produktów, które umożliwiają na warunkach przewidzianych przez Dostawcę udzielenie licencji dla jednostek pozostających w strukturze Zamawiającego.
5. Wykonawca, po zawarciu Umowy, a przed rozpoczęcie korzystania z Produktów, udostępni mechanizmy podpisania umowy licencyjnej z Dostawcą.
6. Na wezwanie Zamawiającego, Wykonawca udostępni link do stron Dostawcy zawierających opis pól eksploatacji oferowanych Produktów oraz zasad ich używania wraz ze zobowiązaniami Dostawcy w zakresie ochrony danych.
7. Dostarczone oprogramowanie instalowane u Zamawiającego musi pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi lub serwerami (np. w przypadku wymiany lub uszkodzenia sprzętu).
8. Zamawiający wymaga możliwości instalacji subskrypcyjnego oprogramowania klienckiego na 5-ciu komputerach klasy PC, 5-ciu tabletach oraz 5-ciu urządzeniach typu smartphone dla każdego uprawnionego licencjonowaniem użytkownika bez ponoszenia dodatkowych opłat.
9. Oferowane pakiety subskrypcji usług hostowanych w chmurze publicznej jej producenta (Dostawcy) muszą zapewniać posiadanie powszechnie uznanych i rozpowszechnionych standardów i norm potwierdzonych aktualnymi wynikami niezależnych audytów, oraz list kontrolnych w szczególności:

a) PN-ISO/IEC
   i. 27001,
   ii. 27002,
   iii. 27017,
   iv. 27018,
   v. 20000-1:2011,
   vi. 22301,
b) SOC 1, SOC 2, SOC 3,
c) Open Authentication Standard – OAuth,
d) CIS Benchmark.

10. Zgodność algorytmów zabezpieczających dane usług platformy hostowanej Dostawcy z FIPS 140.
11. Oferowane pakiety subskrypcji powszechnie dostępnych, standardowych usług muszą zapewniać lub umożliwiać zapewnienie:
    a) Dostępność usług na poziomie 99,9% (lub wyższym),
    b) Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach.
    c) 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 posiadanymi przez Dostawcę.
    d) Możliwość automatycznej, niewpływającej na ciągłość pracy systemów instalacji poprawek dla wybranych składników pakietów usług,
    e) Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
    f) Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi zarządzania tożsamością będącej składową pakietów usług oferowanych przez Dostawcę.
    g) Możliwość realizacji bezpiecznego uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
    h) Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
    i) 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”.
    j) Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych.
    k) Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN).
    l) Możliwość zestawienia (za dodatkową opłatą) dedykowanego połączenia pomiędzy lokalną infrastrukturą sprzętową Zamawiającego, a Centrami przetwarzania Dostawcy,
    m) Możliwość korzystania w ramach pakietów usług Dostawcy z dedykowanych urządzeń typu HSM zgodnych z FIPS 140-2 poziomu 3.
    n) Wbudowane w platformę Dostawcy mechanizmy zabezpieczające przez atakami DDoS,
    o) Możliwość zastrzeżenia miejsca uruchomienia usług i składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego (EOG).
    p) Możliwość korzystania z przynajmniej dwóch równorzędnych centrów przetwarzania danych Dostawcy, składających się z przynajmniej trzech redundantnych ośrodków przetwarzania i położonych na obszarze EOG.

q) Dostępność zapisów umownych Dostawcy zawierających tzw. Klauzule Umowne opublikowane przez Komisję Europejską w zakresie ochrony danych osobowych,
r) Zobowiązania umowne Dostawcy potwierdzające zgodność z rozp. RODO i potwierdzające rolę Dostawcy jako przetwarzającego dane,
s) Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
t) Gwarancję usunięcia danych Zamawiającego z usług i centrów przetwarzania Dostawcy po zakończeniu umowy.
u) Gwarancję braku dostępu do danych Zamawiającego przez Dostawcę, z wyłączeniem działań serwisowych i wykonywanych wyłącznie przez uprawnione osoby z organizacji Dostawcy.

12. Licencjonowanie oprogramowania musi gwarantować prawo instalacji najnowszej wersji oprogramowania klienckiego, będącego przedmiotem zamówienia, dostępnej w trakcie trwania umowy.
13. Zamawiający wymaga zagwarantowania niezmienności cen jednostkowych na zaoferowane Produkty subskrypcyjne dla realizacji zamówień opcjonalnych w całym okresie trwania umowy, z wyłączeniem zmian kursowych EUR/PLN.
14. Zamawiający wymaga oferty zawierającej Produkty, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, aktywacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego oraz jednolitych mechanizmów wykorzystania tożsamości cyfrowej. Udostępnionych przez Dostawcę.
15. Zamawiający wymaga zaoferowania subskrypcji w programie licencyjnym gwarantowanym przez Dostawcę, umożliwiającym w okresie trwania umowy instalację dodatkowych subskrypcji oprogramowania z zamawianego zakresu Produktów z rozliczaniem się za nie post factum - raz do roku.
16. Wykonawca zapewni dostęp do spersonalizowanej strony Dostawcy pozwalającej upoważnionym osobom ze strony Zamawiającego na:
    a) Pobieranie zakupionego oprogramowania,
    b) Aktywację zakupionego oprogramowania,
    c) Sprawdzanie liczby zakupionych Produktów w wykazie zakupionych Produktów.
17. Zamawiający wymaga udzielenia przez Wykonawcę uprawnień na stronie Dostawcy w terminie do 10 dni roboczych od podpisania umowy.
18. Po 120-stu dniach od zakończenia okresu trwania umowy, o ile strony nie postanowią inaczej, Wykonawca zapewni możliwość wyłączenia konta Zamawiającego na spersonalizowanej stronie Dostawcy i usunięcie danych Zamawiającego z centrów przetwarzania Dostawcy.
19. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany Produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym.
20. 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.

1.3. Warunki równoważności - specyfikacja techniczno-eksploatacyjna i cech użytkowych Produktów.

W poniższej części przedstawione są wymagania funkcjonalne dotyczące zamawianych Produktów.

W związku z użyciem przez Zamawiającego w trybie art. 99 ust 5 Pzp opisu przedmiotu zamówienia przez wskazanie znaków towarowych przy jednoczesnym dopuszczeniu rozwiązań równoważnych wobec opisanych w SWZ:

1. Zamawiający wymaga od wykonawców którzy oferują rozwiązania równoważne jednocześnie:
    a) identyfikacji w treści oferty oferowanego produktu równoważnego w sposób i na poziomie szczegółowości określonym w SWZ,
    b) potwierdzenia równoważności zaoferowanych produktów - poprzez wypełnienie formularza oferty i wykazanie, że zaoferowany asortyment spełnia wszystkie opisane w SWZ kryteria oceny równoważności zgodnie z art. 99 ust 6 Pzp,
    c) złożenia wraz z ofertą w charakterze treści oferty po jednym egzemplarzu wskazanego przedmiotu dostawy. W odniesieniu do oprogramowania mogą zostać dostarczone licencje lub subskrypcje tymczasowe, w pełni zgodne z oferowanymi.
2. Zamawiający dokonywał będzie weryfikacji równoważności dostarczonego oferowanego oprogramowania poprzez sprawdzenie ich pełnej zgodności z wymaganiami określonymi w SWZ. Sprawdzenie będzie polegać na wielokrotnym przeprowadzeniu testów w warunkach produkcyjnych w ramach istniejącego systemu opartego o wymienione pakiety oprogramowania i subskrypcji, z użyciem urządzeń peryferyjnych Zamawiającego, na arkuszach, bazach danych i plikach Zamawiającego z dołączeniem do usługi katalogowej Zamawiającego – Active Directory.
3. Negatywny wynik sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 226 ust. 1 pkt. 5 Pzp – z powodu niezgodności treści oferty z warunkami zamówienia.
4. Niezłożenie wraz z ofertą, w przypadku oferowania produktów równoważnych, wymaganych produktów skutkować będzie odrzuceniem oferty zgodnie z art. 226 ust 1 pkt 5 Pzp. Uwzględniając charakter dowodów równoważności jako treści oferty nie podlegają one procedurze uzupełniania.
5. Po przeprowadzeniu weryfikacji, dostarczone do testów produkty zostaną zwrócone wykonawcy.
6. Zamawiający zastrzega sobie także możliwość odwołania się w trakcie procesu weryfikacji równoważności do oficjalnych, publicznie dostępnych stron internetowych producenta weryfikowanego przedmiotu oferty.

1.3.1. M365 E5 Unified Sub Per User

Pakiet subskrypcji usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego musi zawierać następujące oprogramowanie i usługi:

System operacyjny klasy desktop

1. Interfejs graficzny użytkownika pozwalający na obsługę:

a. Klasyczną przy pomocy klawiatury i myszy,

b. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,

2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, zarządzanie systemem, zarządzanie plikami, zarządzanie tożsamością użytkownika, zarządzanie połączeniami, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe, narzędzia aktualizacji.
4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
5. Wbudowany mechanizm geolokalizacji z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
6. Wbudowany system pomocy w języku polskim;
7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
8. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
9. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne,
10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
11. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
12. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
13. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu

operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,

21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
22. Obsługa standardu NFC (near field communication),
23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
26. Mechanizmy uwierzytelniania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
    d. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PIN'u. Mechanizm musi być ze specyfikacją FIDO.
27. Wsparcie dla mechanizmów wieloskładnikowego uwierzytelniania.
28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
30. Wsparcie dla algorytmów Suite B (RFC 4869)
31. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji,
32. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
33. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym,
34. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny,
35. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0,
36. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji,
37. Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu,
38. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,

39. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
40. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
41. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
42. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
43. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning)
44. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
45. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
46. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
47. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
48. Udostępnianie wbudowanego modemu,
49. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
50. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
51. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
52. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
53. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
54. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
55. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikro chipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
56. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
57. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
58. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
59. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),

60. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie
61. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
62. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
63. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
64. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
65. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC oraz pomiędzy dwoma różnymi politykami.
66. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
67. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
68. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
69. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
70. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
71. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache”.
72. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji
73. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
74. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
75. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.

76. Funkcjonalność umożliwiająca na zaktualizowanie systemu bez potrzeby aktualizacji lub przebudowywania paczek aplikacji.
77. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
78. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
79. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym.
80. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
81. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet.
82. Funkcjonalność synchronizacji ustawień aplikacji pomiędzy wieloma komputerami.

Wymagania dotyczące pakietu subskrypcji usługi dostawcy usług cyfrowych (Dostawcy):

1. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Android, Windows lub Apple iOS w najnowszej dostępnej wersji.
2. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
3. 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.
4. Wbudowana usługa zarządzania tożsamością użytkowników musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
5. Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
6. 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”.
7. Gwarantowana dostępność usług na poziomie 99,9%,
8. Możliwość dodawania własnych nazw domenowych.
9. Dostępność portalu administracyjnego do zarządzania usługą oraz zasadami grup.
10. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
11. Ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day.
12. Szyfrowanie danych przesyłanych za pomocą sieci publicznych.
13. Zastosowanie powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy, między innymi Open Authentication Standard – OAuth.
14. Dostępność na żądanie wyników aktualnych wyników audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z uzyskanymi certyfikatami, przynajmniej:

- ISO/IEC 27001, 27002, 27017, 27018,
- ISO/IEC 20000-1,
- ISO/IEC 22301,
- SOC 1, SOC 2, SOC 3,
- CIS Benchmark.

15. Dostępność raportów zgodności z WCAG.
16. Dostępność raportów zgodności z EN 301 549.
17. Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy.
18. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
19. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
20. Wbudowane mechanizmy zabezpieczające przez atakami DDoS,
21. Przynajmniej dwa równorzędne ośrodki przetwarzania danych świadczące Usługę, odległe od siebie o co najmniej 100 km.
22. 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.
23. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
24. 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.
25. Zobowiązania umowne potwierdzające zgodność z rozp. RODO i potwierdzające rolę operatora usługi jako przetwarzającego dane,
26. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
27. Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.

Usługa poczty elektronicznej on-line musi spełniać następujące wymagania:

Usługa musi umożliwiać:

a. obsługę poczty elektronicznej,
b. zarządzanie czasem,
c. zarządzanie rezerwacją zdefiniowanych zasobów,
d. zarządzanie kontaktami i komunikacją.

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 hostowana poczty.

Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:

- Oprogramowania Microsoft Outlook w najnowszej dostępnej wersji,
- Przeglądarki (Web Access),
- Klienta poczty urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 100 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa najnowszych dostępnych funkcji Microsoft Outlook, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla 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:
    - 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.
2. 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 i wiadomości błyskawicznych.
- Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane 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.
- Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
- Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów
- Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.

3. 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 kwot na rozmiar 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 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.
   - 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.

4. 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 PDA, SmartPhone
   - 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, 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) Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0
    a. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
    b. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
    c. 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 narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML,
    c. Wsparcie dla ASP.NET, Apache, C#, Java i PHP,
    d. 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. 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 2019 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 2019, 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:

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 2019.

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

1. Bezpieczną komunikację głosową oraz video,
2. Przesyłanie wiadomości błyskawicznych (tekstowych),
3. Możliwość organizowania telekonferencji,
4. Możliwość przesyłania strumieniowego prezentacji video i głosowej,
5. Możliwość współdzielenia dokumentów w trakcie spotkań on-line (zdalnych),
6. Możliwość definiowania przestrzeni współpracy zespołowej.

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 zapraszania do spotkań zdalnych użytkowników zewnętrznych nieposiadających licencji usługi.
4. Możliwość oceny jakości komunikacji głosowej i wideo.
5. Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze.
6. Dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką UKW lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub wybranych urządzeń stacjonarnych typu telefon IP, kamera dookólna czy duże monitory lub projektory.
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 stworzenia poczekalni dla dołączających użytkowników z dołączaniem ich decyzją uprawnionych osób.
10. Możliwość zastąpienia tła lub jego rozmycia w przypadku transmisji video.
11. 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.

12. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.
13. Możliwość (w przypadku nabycia odpowiednich licencji) realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
14. Możliwość nagrywania telekonferencji przez uczestników z zapisem nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
15. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
16. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
17. Dostępność aplikacji klienckiej usługi UKW (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,
        - Ankiet,
        - Udostępniania plików i pulpitów,
        - Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,
    b. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
    c. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z UKW.

Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 5 TB dla każdego użytkownika. Repozytorium musi umożliwiać użytkownikom pakietów biurowych na:

- traktowanie go, jako własnego dysku,
- synchronizację zawartości wybranego folderu ze stacji roboczej do repozytorium przypisanego danemu użytkownikowi na bazie niezaprzeczalnego uwierzytelnienia,
- 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 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 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 2019 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 najechaniu znacznikiem myszy na dany rodzaj wykresu).

p. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2019, 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:

a. Przygotowywanie prezentacji multimedialnych, które będą:

i. Prezentowanie przy użyciu projektora multimedialnego

ii. Drukowanie 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 MS PowerPoint 2019.

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:

b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.

c. Relacji pomiędzy tabelami

d. Formularzy do wprowadzania i edycji danych

e. Raportów

f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych

g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów

h. 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 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:

   i. Dołączania do telekonferencji,

   ii. Szczegółowej listy uczestników,

   iii. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,

   iv. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,

   v. Głosowania,

   vi. Udostępniania plików i pulpitów,

   vii. 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 wybranych urządzeń peryferyjnych.

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.

Dodatkowo pakiet musi zawierać:

1. Centrum administracyjne pozwalające konfigurować swoją organizację w chmurze, zarządzanie użytkownikami i subskrypcjami i umożliwiać resetuj hasła.
2. Obsługa konfiguracji danych diagnostycznych systemu operacyjnego, zapewniającą kontrolę nad danymi diagnostycznymi.
3. Zarządzanie urządzeniami z systemem Windows, w tym dostęp warunkowy,
4. Usługę wglądu i analizy w celu podejmowania decyzji dotyczących gotowości do aktualizacji systemów Windows.
5. Usługę zarządzania chmurą (cloud management gateway) zapewniającą zarządzanie konfiguracjami klienckimi przez Internet, bez ujawniania infrastruktury lokalnej w Internecie.
6. Zarządzanie instalacją i aktualizacją aplikacji klienckich pakietu.
7. Konfigurowanie zasad bezpiecznego dostępu użytkowników do zasobów organizacji (danych i aplikacji) z lokalizacji zdalnych, obejmujące między innymi profile sieci Wi-Fi, sieci VPN, poczty e-mail i certyfikatów.
8. Zarządzanie zasadami ochrony przed złośliwym kodem i zabezpieczeniami zapory dla komputerów klienckich.
9. Zbieranie i raportowanie informacji o plikach przechowywanych na komputerach klienckich w organizacji.
10. Tworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania w ramach systemów Zamawiającego i poza nimi, chroniąc ją przed nieuprawnionym dostępem. Usługa musi spełniać następujące wymagania:
    1) Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,
    2) Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
    3) Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
    4) Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
    5) Możliwość klasyfikacji informacji i ustalania szablonów tej klasyfikacji.
    6) Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, w tym:
        a. Brak uprawnień dostępu do informacji,
        b. Informacja tylko do odczytu,
        c. Prawo do edycji informacji,
        d. Brak możliwości wykonania systemowego zrzutu ekranu,
        e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,

f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,

g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.

7) Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,

8) Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji,

9) Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji,

10) Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,

11) Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

12) Scentralizowane zarządzanie przydzielania dostępu do aplikacji,

13) Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),

14) Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),

15) Samoobsługowe resetowania hasła.

16) Dostarczanie mechanizmów usługi uwierzytelniania użytkowników,

17) Konsolę zarządzania tożsamością i dostępem.

11. Zarządzanie aplikacjami mobilnymi, które ma na celu ochronę danych organizacji na poziomie aplikacji, w tym aplikacji niestandardowych i aplikacji sklepowych. Zarządzanie aplikacją ma być używane na urządzeniach należących do organizacji i na urządzeniach osobistych. Zarządzanie ma umożliwiać:

    a. Dodawanie i przypisywanie aplikacji mobilnych do grup użytkowników i urządzeń, w tym użytkowników w określonych grupach, urządzeń w określonych grupach.

    b. Konfigurowanie, uruchamianie lub uruchamianie aplikacji z określonymi ustawieniami i aktualizację aplikacji już zainstalowanych na urządzeniu.

    c. Dostarczanie raportów dotyczących używanych aplikacji i ich użycia.

    d. Czyszczenie selektywne, usuwające z aplikacji tylko dane organizacji.

12. Oprogramowanie pozwalające na wykrycie zagrożeń i anomalii działań użytkowników oraz zaistniałej penetracji systemów.

    1) Wymagane jest oprogramowanie pozwalające analizować, poznawać i identyfikować typowe i nietypowe zachowania użytkowników, urządzeń, aplikacji i wszelkich zasobów.

    2) Wbudowana baza wzorców działania typowych komponentów systemu pozwalająca wykryć typowe efekty ataku na system.

    3) Wbudowane mechanizmy uczenia się – pozwalające rozpoznawać nietypowe zachowania i zdarzenia będące odstępstwami od normalnego działania systemów.

    4) Współdziałanie z Serwerowym systemem operacyjnym z elementami zarządzania.

    5) Wykrywanie i raportowanie zdarzeń takich jak:

    6) Nietypowe zmiany w DNS

7) Masowe zmiany w prawach dostępu,
8) Nieoczekiwane zmiany na poziomie usługi LDAP,
9) Dostęp do zasobów bez posiadania uprawnień,
10) Posługiwanie tymi samymi uprawnieniami przez wielu użytkowników,
11) Wielokrotne nieudane próby dostępu,
12) Aktywności na poziomie mechanizmów Honeypot i Honeytoken,
13) Nietypowe zachowania użytkowników,
14) Masowe kasowanie obiektów czy informacji,
15) Wykrywanie typowych niedociągnięć w konfiguracji czy procedurach, takie jak brak szyfrowania, przechowywanie haseł w postaci tekstu.

13. Dziennik inspekcji w centrum zgodności z ustanowionymi zasadami ochrony informacji, pozwalający na sprawdzenie, czy użytkownik przeglądał określony dokument lub usuwał określony element ze skrzynki pocztowej.
14. Tworzenie syntetycznego wskaźnika stanu zabezpieczeń organizacji, pozwalającego na:
    a. Monitorowanie zabezpieczeń pakietu, aplikacji i urządzeń,
    b. Raportowanie bieżącego stanu zabezpieczeń organizacji,
    c. Poprawianie stanu bezpieczeństwa dzięki możliwości odnajdowania komponentów źle zabezpieczonych,
    d. Porównanie wskaźników bezpieczeństwa z wzorcami i ustalanie kluczowych wskaźników dla bezpieczeństwa (KPI).
15. Rozbudowane funkcje zarządzania tożsamością użytkowników, które:
    1) Umożliwia użytkownikom rozwiązań hybrydowych wykorzystanie ich tożsamości cyfrowej dla systemów własnych (on premis) i w chmurze,
    2) Pozwala na zaawansowaną administrację użytkownikami poprzez tworzenie grup zarządzania i mechanizmy samoobsługi dla grup,
    3) Samoobsługę użytkowników w zakresie resetu hasła w systemach własnych,
    4) Samoobsługę użytkowników w zakresie dołączania do usługi,
    5) Narzędzie do zarządzania tożsamością cyfrową i prawami dostępu w systemach własnych,
    6) Narzędzia uwierzytelniania wieloskładnikowego,
    7) Zawiera mechanizmy ochrony tożsamości cyfrowej pozwalającej określać zasady dostępu warunkowego do danych i aplikacji,
    8) Mechanizmy generycznej klasyfikacji danych,
    9) Zaawansowane raporty na temat odstępstw od zasad bezpieczeństwa,
    10) Automatycznej detekcji zagrożeń i redukcji związanego z tym ryzyka,
    11) Detekcji zagrożonych kont,
    12) Analizy ryzyk i udostępniania danych na temat wykrytych ryzyk,
    13) Warunkowego dostępu na bazie analiz czynników nietypowych,
    14) Narzędzia pozwalające na detekcję i monitorowanie kont o uprzywilejowanym dostępie.

16. Pakiet zaawansowanej ochrony musi umożliwiać wykrywanie, zapobieganie, analizę i przeciwdziałania zagrożeniom. Pakiet subskrypcji musi:
    1) Umożliwiać definiowanie polityk ochrony przed cyberzagrożeniami wraz ustaleniem odpowiedniego poziomu tych zabezpieczeń.
    2) Kreować raporty o działaniu tego pakietu w czasie rzeczywistym.
    3) Raportować wykryte zagrożenia, analizować phishingowe adresy i wiadomości.
    4) Wykrywać, opisywać i symulować cyberzagrożenia dla Office 365 wraz z możliwością automatyzacji podstawowych działań.
    5) Eliminować rozpoznane w monitoringu Dostawcy typy zagrożeń.
    6) Sprawdzać bezpieczeństwo załączników poczty elektronicznej poprzez otwieranie ich i skanowanie zawartości w chronionych środowiskach wirtualnych.
    7) Sprawdzać bezpieczeństwo linków zawartych w poczcie elektronicznej poprzez otwieranie ich i skanowanie zawartości w chronionych środowiskach wirtualnych.
    8) Sprawdzać bezpieczeństwo plików składowanych w SharePoint Online i Teams poprzez otwieranie ich i skanowanie zawartości w chronionych środowiskach wirtualnych.
    9) Pozwalać na uruchamianie anti-phishingowych polityk sprawdzających zgodność domeny nadawcy.
    10) Pozwalać na tworzenie list bezpiecznych i niebezpiecznych domen.
    11) Pozwalać na definiowanie standardowych działań na podejrzanych wiadomościach.
    12) Umożliwiać włączanie mechanizmów sztucznej inteligencji wykrywającej nietypowe wzorce wiadomości.
    13) Analizować rozpoznane typy ataków, które mogą spowodować zagrożenia.
    14) Automatyzować działania rozpoznawania i zapobiegania atakom.
    15) Udostępniać symulacje ataków dla celów treningu zespołów bezpieczeństwa.
    16) Wspomagać podejmowanie decyzji w przypadku ataku.
17. Narzędzia umożliwiające wykrywanie, zapobieganie, analizę i przeciwdziałania zagrożeniom. Pakiet oprogramowania musi:
    1) Zapewniać ochronę antywirusową w czasie rzeczywistym.
    2) Aktualizować wzorce zagrożeń oraz zasady blokowania złośliwego oprogramowania.
    3) Umożliwiać uruchamianie skanowania, izolowania, objęcia kwarantanną zagrożonych urządzeń i oznaczania/blokowania niebezpiecznych plików.
    4) Ograniczać powierzchnię potencjalnych ataków.
    5) Udostępniać portal z aktualną informacją o wykrytych zagrożeniach, zarządzać ustawieniami ochrony wraz z kreowaniem raportów na te tematy i podejmować akcje eliminujące zagrożenia.
    6) Wprowadzać dostęp zależny od roli użytkownika systemu ochrony.
    7) Udostępniać wieloplatformowe API dla automatyzacji procesów związanych z ochroną zasobów.
    8) Dzięki analizie danych wielu urządzeń i poznanych typach ataków identyfikować typ zagrożenia sygnalizując je w alertach.

9) Redukować powierzchnię ataku poprzez wskazywanie właściwej konfiguracji urządzenia i systemu operacyjnego oraz ograniczanie dostępu do znanych jako niebezpieczne adresów IP, domen czy linków.
10) Wskazywać operatorom SOC najważniejsze zagrożenia i rekomendowane działania.

18. Broker zabezpieczeń dostępu do chmury, identyfikujący i zwalczający cyberzagrożenia w usługach w chmurze, który zapewnia wielofunkcyjny wgląd, kontrolę nad przenoszeniem danych i zaawansowaną analizę.
19. Narzędzie kontroli spełniania wymagań w zakresie zgodności dotyczące wielu wykorzystywanych chmur, w ramach przepisów i standardów globalnych, branżowych lub regionalnych.
20. Obsługa sterowania połączeniami i funkcje centrali PBX w chmurze w ramach usługi komunikacji wielokanałowej zawartej w pakiecie.

1.3.2. Project Plan3 Shared All Lng Subs VL MV L Per User

Pakiet subskrypcji zarządzania projektami musi spełniać następujące wymagania i funkcje:

1. Możliwość wyboru jeżyka interfejsu użytkownika, w tym języka polskiego i angielskiego.
2. Implementacja przyjętych w skali organizacji procedur zarządzania projektami. Planowanie, śledzenie i kontrola realizacji projektów muszą odbywać się w oparciu o procedury przyjęte w ramach własnych doświadczeń projektowych. Wymagana jest implementacja rozwiązania umożliwiającego śledzenie realizowanych projektów, postępów prac, obciążenia zasobów, kontrolę kosztów etc.
3. Współdziałanie z kalendarzami systemu Exchange w zakresie przepływu informacji o zadaniach i ich aktualizacji, z wyłączeniem informacji typu out-of-office (poza biurem).
4. Wykorzystanie otwartego standardu OData do wyszukiwania danych i ich analizy.
5. Dane dotyczące realizowanych projektów i dokumentacja projektowa muszą być przechowywane w sposób bezpieczny z ochroną dostępu dla uprawnionych osób. System ma umożliwić dostęp do aktualnego statusu prowadzonych projektów.
6. Możliwość wykorzystania profili użytkowników lub ich grup z usługi katalogowej przy udzielaniu uprawnień dostępu.
7. Kontrola, rozpatrywanie i zatwierdzanie dokumentów za pomocą definiowalnego przepływu pracy (workflow),
8. Możliwość definiowania przepływu pracy przy pomocy oprogramowania Visio.
9. System zarządzania projektami:
    a. szybki wgląd w aktualny status realizowanych projektów,
    b. określenie kosztów ponoszonych w poszczególnych projektach,
    c. ocenę prac w zakresie zgodności z harmonogramem i przyjętym budżetem,
    d. określenie zasobów zaangażowanych w realizację poszczególnych projektów i poziomu ich zaangażowania,
    e. określenie odpowiedzialności za realizację poszczególnych zadań i projektów,

f. aktualną ocenę stanu dostępności zasobów w organizacji.

10. Dostęp do funkcji systemu poprzez przeglądarkę Edge, Firefox, Safari i Chrome.
11. Możliwość definiowania projektów za pomocą pakietu zarządzania projektami (niezależnego narzędzia instalowanego na stacjach klienckich).

Usługa ma udostępniać poszczególnym grupom odbiorców różne cechy i funkcjonalność.

1. Zarządzanie projektami

System zarządzania projektami ma zapewnić sprawną koordynację i zarządzanie projektami. Dzięki Centralnemu Repozytorium Projektów (CRP), kierownictwo ma utrzymywać oraz wdrażać szablony planów projektów. Zarządzanie projektami ma zapewnić uzyskanie jednolitych raportów przedstawianych przełożonym oraz instytucjom zewnętrznym, w tym jednostkom prowadzącym audyty projektów.

Wymagane informacje o Projekcie

a. Definiowanie inicjatyw projektowych,
b. Definiowanie typów projektów dla wszystkich żądań i możliwość powiązania ich z cyklami pracy, planem projektu i zindywidualizowanymi szablonami miejsca pracy.
c. Przygotowanie harmonogramów,
    - Opis listy zadań do wykonania
    - Określenie struktury hierarchicznej zadań (WBS)
    - Określenie zależności między zadaniami – relacje,
d. Zapisywanie projektów do centralnego repozytorium,
e. Przygotowanie szablonów harmonogramów i opublikowanie ich do repozytorium szablonów,
f. Automatyczne przekształcanie inicjatyw projektowych w projekty przy wykorzystaniu szablonów projektowych,
g. W zależności od wybranych kategorii dla inicjatywy projektowej, tworzony projekt powinien zawierać harmonogram charakterystyczny dla danego typu projektu,
h. Przeglądanie informacji o projektach za pomocą przeglądarki internetowej,
i. Grupowanie projektów według zadanych kryteriów,
    - Etap projektu,
    - Lokalizacja projektu,
    - Kierownik projektu,
    - Itp.
j. Sygnalizacja graficzna opóźnienia zadania względem planu bazowego
    - Informacja czy jest plan bazowy,
    - Informacja o odchyleniu względem czasu,
    - Informacja o odchylenia względem kosztu,
    - Informacja o odchyleniach względem pracy,
k. Śledzenie postępu realizacji projektu
    - Analiza czasu,

- Analiza kosztu,
- Analiza godzin przepracowanych,

l. Raportowanie
   - Informacja o zadaniach opóźnionych,
   - Informacja o kosztach zadań,
   - Informacja o pracy w zadaniach,

m. Delegowanie uprawnień do projektu,

n. Zmiana właściciela projektu,

o. Dynamiczna zmiana właściciela projektu, zgodnie z wyborem kierownika projektu,

p. Kontrola zmian pól opisujących projekt – zmianę pól może dokonywać tylko administrator lub biuro projektów,

1.3.3. VisioPlan2 ShrdSvr ALNG SubsVL MVL PerUsr

Pakiet subskrypcji usług do graficznego modelowania w postaci wektorowej: procesów biznesowych, procesów obiegu informacji, schematów organizacyjnych, diagramów sieciowych, harmonogramów wraz możliwością instalacji pakietu na komputerze klasy PC.

Pakiet musi zapewniać:

1. Możliwość otwierania i przeglądania rysunków przy użyciu bezpłatnie dostępnego narzędzia.
2. Zgodność z interfejsem dotykowym Windows.
3. Możliwość pracy kilku osób na jednym diagramie w tym samym czasie.
4. Zapis danych w postaci plików XML.
5. Zgodność ze standardami:
6. Unified Modeling Language (UML) 2.4,
7. Business Process Model and Notation (BPMN) 2.0.
8. Publikacja przepływów pracy dla SharePoint.
9. Możliwość importu i eksportu do formatu plików zgodnych z AutoCad.
10. Możliwość graficznego obrazowania i analizowania danych pobieranych z plików xls i xlsx, baz danych dostępnych przez ODBC na diagramach.
11. Udostępnianie kreatorów budowy diagramów.
12. Udostępnianie gotowych kształtów (shape) opisanych metadanymi i możliwość kreowania i edycji kształtów.
13. Możliwość zmiany kształtu przy zachowaniu jego metadanych oraz całości diagramu.
14. Możliwość budowy diagramów przestawnych, które są kolekcją kształtów uporządkowanych w strukturę drzewa, która pomaga analizować dane i podsumowywać je w zrozumiałym formacie wizualnym. Taki diagram zaczyna się od kształtu nazywanego węzłem najwyższego poziomu, który zawiera informacje zaimportowane z arkusza, tabeli, widoku lub modułu.

Węzeł najwyższego poziomu można podzielić na poziom węzłów podrzędnych, aby dane można było wyświetlać w różny sposób.

15. Udostępnianie gotowych szablonów służących do wizualizowania i usprawniania procesów biznesowych, śledzenia projektów i zasobów, układania schematów organizacji, mapowania sieci, tworzenia diagramów obszarów budowy i optymalizacji systemów. Wymagane są szablony graficznego modelowania w postaci wektorowej:
    - procesów biznesowych,
    - procesów obiegu informacji,
    - schematów organizacyjnych,
    - diagramów sieciowych,
    - harmonogramów.
16. Funkcja autołączenia, która automatycznie łączy kształty, równomiernie je rozmieszcza i wyrównuje do założonej siatki. Przenoszenie połączonych kształtów nie rozłącza ich, tylko powoduje automatyczne wytyczenie nowej trasy łącznika między nimi.
17. Połączenie diagramów z danymi umożliwiające uzyskanie obrazu procesu, projektu lub systemu pozwalające na identyfikowanie kluczowych trendów, problemów i wyjątków, a następnie określanie właściwego sposobu postępowania.
18. Graficzne raporty z informacjami o projektach do wizualizacji kompleksowych informacji o projektach. Umożliwienie generowania raportów, które pozwalają śledzić informacje o zadaniach, właścicielach, rolach i obowiązkach dotyczących projektów, a także przedstawiają złożone struktury własności w projekcie.
19. Możliwość automatycznego modyfikowania raportów w miarę zmian informacji o projektach.

1.3.4. M365 F3 FUSL Sub Per User

Subskrypcja usług komunikacyjnych, bezpieczeństwa i oprogramowania klasy desktop (subskrypcja na użytkownika)

Pakiet subskrypcji usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego (on-line) typu COTS (Commercial Of-The-Shelf) ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line – usługi katalogowej typu LDAP, portalu wewnętrznego, poczty elektronicznej, narzędzi wiadomości błyskawicznych, konferencji głosowych i video, repozytorium dokumentów, wewnętrznego serwisu społecznościowego oraz edycji dokumentów biurowych on-line (dalej Usługi). Dodatkowo subskrypcja pakietu ma uprawniać do instalacji systemu operacyjnego klasy desktop i wykorzystania usług bezpieczeństwa.

Wymagania dotyczące pakietu subskrypcji usługi:

1. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Android, Windows lub Apple iOS w najnowszej dostępnej wersji.
2. Możliwość instalacji aplikacji dostępowych dla jednego użytkownika - na 5-ciu komputerach klasy PC, 5-ciu tabletach i 5-ciu smartfonach.

3. 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.

Usługa poczty elektronicznej on-line musi spełniać następujące wymagania:

Usługa musi umożliwiać:

a. obsługę poczty elektronicznej,
b. zarządzanie czasem wraz z zarządzaniem dniem pracy i harmonogramowaniem,
c. pracę zespołową w zintegrowanym środowisku udostępniania dokumentów, rozmów błyskawicznych, dyskusji,
d. publikacji kontentu w tym materiałów multimedialnych,
e. zarządzanie kontaktami i komunikacją.

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 hostowana poczty.

Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:

- Posiadanego oprogramowania klienckiego obsługującego protokół POP,
- Przeglądarki (Web Access),
- Urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 2 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Wsparcie dla Internet Explorer, 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:

Funkcjonalność podstawowa:

1. 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.

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

Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań

Obsługa list i grup dystrybucyjnych.

Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności,

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.

Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.

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

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

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

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.

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.

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

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 PDA, SmartPhone

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 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) Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0
    a. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
    b. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
    c. 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 narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML,
    c. Wsparcie dla ASP.NET, Apache, C#, Java i PHP,
    d. 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

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:

7. Wymagania odnośnie interfejsu użytkownika:
    a. Pełna polska wersja językowa interfejsu użytkownika,
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych

8. 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)
9. 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.
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. Wstawianie oraz formatowanie tabel
    c. Wstawianie oraz formatowanie obiektów graficznych
    d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
    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. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
    k. Określenie układu strony (pionowa/pozioma)
    l. Wydruk dokumentów
    m. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
    n. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010 i 2016z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
    o. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
    p. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.

q. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

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. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
    j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
    k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
    l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
    m. 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.
    n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

12. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    a. Przygotowywanie prezentacji multimedialnych, które będą:
    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.

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

7. Bezpieczną komunikację głosową oraz video,
8. Przesyłanie wiadomości błyskawicznych (tekstowych),
9. Możliwość organizowania telekonferencji,
10. Możliwość współdzielenia dokumentów w trakcie spotkań on-line (zdalnych).

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

18. 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.
19. 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.
20. Możliwość oceny jakości komunikacji głosowej i wideo.
21. 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.
22. 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.
23. Dostępny kliencki sprzęt peryferyjny różnych producentów posiadający potwierdzenie zgodności z SKW przez producenta SKW.
24. 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.
25. 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.
26. Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.
27. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.

28. Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
29. Możliwość nagrywania telekonferencji przez uczestników.
30. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
31. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
32. Wbudowane funkcjonalności: SIP Proxy.
33. Wbudowana funkcjonalność mostka konferencyjnego MCU.
34. Obsługa standardów: CSTA, TLS, SIP over TCP.
35. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
36. Kodowanie video H.264,
37. Wsparcie dla adresacji IPv4 i IPv6,
38. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
39. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników,
40. Możliwość szyfrowania połączeń.
41. 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,
42. 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,

d. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.

e. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

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 licencyjne i nadane przez administratorów:

1. 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 SKW.
2. Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).
3. Współdziałanie mechanizmów SKW z pocztą głosowa, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:
    a. Uruchamiania funkcji komunikacyjnych SKW z wybranych interfejsów klienta poczty elektronicznej, składników pakietu biurowego czy portalu,
    b. Dostępności w tych interfejsach danych o statusie obecności innych użytkowników (np. w nagłówkach poczty elektronicznej, czy listach użytkowników portalu.
    c. 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 2GB dla każdego użytkownika. Repozytorium musi umożliwiać użytkownikom pakietów biurowych na:

- traktowanie go, jako własnego dysku,

- zapis do repozytorium przypisanego danemu użytkownikowi na bazie niezaprzeczalnego uwierzytelnienia,

- synchronizację zawartości repozytorium z wieloma urządzeniami w ramach uprawnień użytkownika –właściciela repozytorium.

System operacyjny klasy desktop

System operacyjny klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

2. Interfejs graficzny użytkownika pozwalający na obsługę:
    a. Klasyczną przy pomocy klawiatury i myszy,
    b. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,

3. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe,
5. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
6. Wbudowany system pomocy w języku polskim;
7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
8. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
9. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
10. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne,
11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
12. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
13. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
14. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
15. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
16. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
17. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
18. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
19. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
20. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
21. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
22. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,

23. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
24. Obsługa standardu NFC (near field communication),
25. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
26. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
27. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
28. Mechanizmy uwierzytelniania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
    d. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.
29. Mechanizmy wieloskładnikowego uwierzytelniania.
30. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
31. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
32. Wsparcie dla algorytmów Suite B (RFC 4869)
33. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji,
34. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
35. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym,
36. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny,
37. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0,
38. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji,
39. Możliwość konfiguracji trybu „kioskowego” dającego dostęp tylko do wybranych aplikacji i funkcji systemu,
40. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
41. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;

42. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
43. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
44. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
45. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning)
46. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
47. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
48. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
49. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
50. Udostępnianie wbudowanego modemu,
51. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
52. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
53. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
54. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
55. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
56. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
57. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
58. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
59. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
60. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
61. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),
62. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie

63. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
64. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
65. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
66. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
67. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
68. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
69. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
70. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
71. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
72. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
73. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
74. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
75. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
76. Funkcjonalność umożliwiająca na zaktualizowanie systemu bez potrzeby aktualizacji lub przebudowywania paczek aplikacji.
77. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
78. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
79. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym.
80. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.

81. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet.
82. Funkcjonalność synchronizacji ustawień aplikacji pomiędzy wieloma komputerami.

Subskrypcja usługi zarządzania urządzeniami oraz tożsamością użytkowników

Subskrypcja pakietu usług zarządzania urządzeniami oraz tożsamością użytkowników musi spełniać następujące wymagania:

Wymagania ogólne

1. Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy,
2. Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym),
3. Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm, w tym zgodności z normami ISO 27017 i 27018,
4. 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.
5. Możliwość skalowania usługi z ustalonymi kosztami takiego skalowania,
6. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
7. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
8. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
9. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
10. 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”.
11. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
12. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
13. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
14. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych,
15. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Unii Europejskiej.
16. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
17. Mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.
18. Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.

19. 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 usługi.

Wymagania funkcjonalne

1. Zarządzanie urządzeniami mobilnymi (iOS, Android, Windows Phone, Windows RT),
2. Możliwość wykorzystania Right Management Services (RMS) - ochronę treści na urządzeniach mobilnych,
3. Portal klasy self-service dla użytkowników mobilnych pozwalający na zdalny reset haseł i zarządzanie przynależnością do grup security w usłudze katalogowej,
4. Podniesienie poziomu bezpieczeństwa dostępu do aplikacji webowych – poprzez uwierzytelnianie wieloskładnikowe (np. poprzez jednorazowe hasła SMS),
5. Prawo do korzystania z rozwiązania klasy on-premise, który służy do zaawansowanego zarządzanie tożsamością w organizacji.

Wymagane scenariusze użycia:

1. 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.
2. Możliwość pracy na prywatnych urządzeniach użytkowników zapewniający bezpieczny i kontrolowany dostęp do danych i aplikacji, w możliwością wydzielenia i usunięcia danych służbowych z urządzenia,
3. Jednokrotne logowanie (single sign-on)w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika, przy zachowaniu niezaprzeczalności działań,
4. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwalający na redukcję ilości zgłoszeń działów wsparcia,
5. 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),
6. Zarządzanie urządzeniami mobilnymi pozwalające na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwiające zdalne kasowanie danych firmowych lub całego urządzenia.

Podsystem zarządzania tożsamością:

System zarządzania tożsamością elektroniczną ma zapewniać pobieranie, agregację oraz synchronizacje danych o użytkownikach z różnych systemów w ramach organizacji wraz z zarządzaniem certyfikatami wydawanymi w ramach własnego centrum certyfikacji (CA).

Bezpieczeństwo

1. System zarządzania tożsamością musi umożliwiać zastosowanie - przy połączeniu ze źródłami danych - mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji).

2. System musi zapewniać prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej zaporami *firewall* oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
3. System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
4. System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.

Skalowalność

5. System zarządzania tożsamością musi umożliwiać skalowanie mechanizmów systemu, pozwalające na obsługę informację w zakresie do 10 000 obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem oraz mieć możliwość skalowania stanowisk wydających certyfikaty.

Interoperacyjność

6. System zarządzania tożsamością musi zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem.
7. System zarządzania tożsamością musi zapewniać możliwość realizacji dwukierunkowej, uprawnionej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.

Skalowalność funkcjonalna

8. System zarządzania tożsamością powinien umożliwiać rozszerzanie funkcjonalności o połączenia z nowymi typami źródeł danych jak i rozszerzenie mechanizmów logiki systemu.
9. System zarządzania tożsamością powinien umożliwiać rozszerzanie rozwiązania o mechanizmy raportowanie i audytu informacji o tożsamości.

Wydajność

10. System musi umożliwiać generowanie i nagrywanie certyfikatów na kartach w liczbie min. xx na godzinę na stanowisko.

Wymagania w zakresie cech i funkcjonalności rozwiązania

1. Agregacja i synchronizacja danych
    a. System musi zapewniać możliwość odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą.
    b. System zarządzania tożsamością, w ramach początkowego wdrożenia musi zapewnić możliwość integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:

- Pliki tekstowe CSV, AVP, LDIF
- Bazy danych MS SQL 2000 - 2016, Oracle
- Usługi katalogowe Microsoft Active Directory, Novell eDirectory, OpenLDAP.

    c. System musi zapewniać możliwość komunikacji z powyższymi informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.

d. System musi zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy integrujące poprzez budowę odpowiedniego rozszerzenia systemu.

e. System musi zapewniać możliwość uprawnionego tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.

f. System musi dostarczać mechanizmy pozwalające na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.

g. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system musi umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium, umożliwiając synchronizację danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.

h. System musi oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.

i. System musi umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.

2. Repozytorium danych teleadresowych

a. System musi umożliwiać agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.

b. System misi zapewnić interfejs użytkownika zapewniający możliwość wyszukiwania oraz przeglądania danych dla wszystkich uprawnionych użytkowników systemu.

c. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie dostępu, zarządzania oraz uaktualnienia danych teleadresowych.

d. W ramach interfejsu użytkownika system musi zapewniać możliwość udostępnienia edycji zakresu udostępnianych danych samodzielnie przez każdego z uprawnionych użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.

3. Zarządzanie kartą elektroniczną

a. Zarządzanie kartami elektronicznymi musi obejmować: personalizację graficzną kart (nadruk), zdalne zarządzania PIN'ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów),

b. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 10 000 użytkowników,

c. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnym przechowywanym i wygenerowanym na karcie)

d. System musi umożliwiać wydawanie i zarządzanie wieloma certyfikatami na jednej karcie (przewiduje się wykorzystanie 4 certyfikatów dla jednego użytkownika)

e. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania itp.,

f. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP,

g. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI,

h. System musi wspierać zarządzanie certyfikatami używanymi do uwierzytelnienia w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.

i. System musi umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów,

j. Po wystawieniu certyfikatu, system musi umożliwić włączenie automatycznej publikacji certyfikatu w katalogu LDAP,

k. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP,

l. Certyfikaty wystawione na jednej stacji muszą być automatycznie dostępne dla użytkownika na innej stacji o ile się tam zaloguje (dotyczy certyfikatów przechowywanych w profilu użytkownika jak i certyfikatów przechowywanych na karcie elektronicznej),

m. Systemu musi posiadać przyjazny interfejs oparty o WWW, przez który użytkownik końcowy może wykonywać operacje zarządzania swoimi certyfikatami i PIN'ami dostępowymi (zmiana PIN'u, odblokowanie karty),

n. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/ wygenerowanie PIN'u inicjującego do karty elektronicznej następującymi drogami:

- Użytkownik lub administrator wprowadza PIN inicjujący,
- PIN inicjujący jest losowo generowany przez system i przekazywany użytkownikowi po autoryzacji na stronie WWW,
- System generuje PIN inicjujący i drukuje go w sposób uniemożliwiający odczytanie go przez osoby postronne bez rozerwania koperty / wydruku,
- PIN może być dostarczony do systemu z zewnętrznego źródła (musi być dostarczone odpowiednie API),

o. Personalizacją graficzna musi pobierać ze wskazanego przez Zamawiającego źródła danych, zdjęcia pracowników i umieszczać je wraz z innymi danymi identyfikacyjnymi na karcie.

p. System musi umożliwiać odblokowanie kart w oparciu o autoryzację użytkownika w katalogu LDAP z wykorzystaniem hasła jednokrotnego,

q. Bezpośrednie odblokowanie karty musi być wykonywane w oparciu mechanizm challenge/response (zabrania stosowania się SO PIN'u statycznego),

r. Na PIN'y wykorzystywane przez użytkownika musi być możliwość nakładania polityk bezpieczeństwa definiujących stopień skomplikowania PIN'u, w szczególności:

- nie mniej niż 6 znaków,

- wymagane cyfry litery małe i duże,
- PIN może się powtarzać przez N zmian,

s. System musi wspierać karty Cryptotech MultiliSign 2.0 lub równoważne,

t. Zarządzanie wystawianiem certyfikatów musi się odbywać w oparciu o definiowalny przepływ roboczy (workflow), który będzie mógł być modyfikowany bezpośrednio przez operatora systemu z poziomu interfejsu graficznego,

u. Workflow musi umożliwiać, implementacji następujących scenariuszy użycia:

- w pełni automatyczne wystawianie certyfikatów dla użytkowników,
- wystawianie certyfikatów wymagające każdorazowej aprobaty operatora systemu,
- automatyczne odświeżanie wybranych certyfikatów,
- automatyczne odtwarzanie wszystkich certyfikatów na kartę elektroniczną w przypadku jej zastąpienia,
- weryfikację czy użytkownik ma odpowiednie certyfikaty lub czy certyfikaty nie wygasają i w razie potrzeby system musi uruchamiać odpowiednią procedurą wystawiania lub wznawiania certyfikatu,
- powiadamianie administratorów systemu o wygasaniu certyfikatów dla serwerów / urządzeń wchodzących w skład infrastruktury teleinformatycznej,

v. Wbudowane workflow musi udostępnić możliwość definiowanie wielu wzorców certyfikatów (w zależności od ich zastosowania) w połączeniu z odpowiednią ścieżką wystawiania/dostarczania certyfikatów do użytkownika, w szczególności:

- certyfikat do szyfrowania poczty wystawiany jest automatycznie o ile użytkownik posiada certyfikat na karcie elektronicznej do podpisu, podpis ten musi być użyty do podpisania wystawianie certyfikatu do szyfrowania,
- certyfikat do logowania jest wystawiony, jeśli użytkownik posiada kartę elektroniczną przypisaną do siebie oraz poprawnie zautoryzuje się hasłem jednokrotnym na stronie WWW systemu,

Definiowanie takich reguł musi być dostępne bezpośrednio dla operatora systemu i nie może wymagać dodatkowych opłat licencyjnych,

w. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, liczby zmian PIN'ow, czy liczby odblokowanych kart,

x. Dane służące do deszyfracji kluczy prywatnych użytkowników przechowywanych w systemie, muszą być bezpiecznie składowane na urządzeniu HSM typu nCipher netHSM 500 lub w pełni równoważnych,

y. Bezpośrednie zarządzania kartami musi odbywać się przez dostarczany wraz z systemem Microsoft Windows interfejs „Microsoft Smart Card Base CSP" lub standard PKCS#11,

z. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania),

Podsystem zarządzania urządzeniami mobilnymi

1. Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:

a. Integrację z systemem Microsoft SCCM w oparciu o natywne interfejsy komunikacyjne
b. Wykorzystanie bazy użytkowników znajdujących się w Active Directory
c. Inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych,
d. Inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji:
    i. Nazwa urządzenia
    ii. Identyfikator urządzenia
    iii. Nazwa platformy systemu operacyjnego
    iv. Wersja oprogramowania układowego
    v. Typ procesora
    vi. Model urządzenia
    vii. Producent urządzenia
    viii. Architektura procesora
    ix. Język urządzenia
    x. Lista aplikacji zainstalowanych w ramach przedsiębiorstwa

2. W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).
3. Wymagania w zakresie dystrybucji oprogramowania:
    a. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
    b. Usługa ma umożliwiać dystrybucję oprogramowania na żądanie użytkownika, realizowane poprzez wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji
    c. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
    d. Katalog aplikacji ma wspierać następujące formaty aplikacji mobilnych:
        i. *. appx (Windows RT)
        ii. *.xap (Windows Phone 8)
        iii. *.ipa (iOS)
        iv. *.apk (Android)
    e. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:
        i. Windows Store
        ii. Windows Phone Store

iii. Android Google Play Store

iv. iOS App Store

4. W obszarze polityki haseł usługa zapewni:
    i. Zdefiniowanie wymuszenia hasła,
    ii. Określenie minimalnej długości hasła,
    iii. Określenie czasu wygasania hasła,
    iv. Określenie liczby pamiętanych haseł,
    v. Określenie liczby prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia,
    vi. Określenie czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła.
5. Usługa ma umożliwiać skorzystanie z szeregu predefiniowane raportów dedykowanych dla klas urządzeń mobilnych. W szczególności w obszarze raportowania zainstalowanego oprogramowania jest możliwość zebrania informacji o zainstalowanym oprogramowaniu na urządzeniu firmowym lub urządzeniu użytkownika:

Podsystem ochrony informacji

Usługa bezpieczeństwa informacji musi pozwalać na stworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania w ramach systemów Zamawiającego i poza nimi, chroniąc ją przed nieuprawnionym dostępem. Usługa musi spełniać następujące wymagania:

1. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,
2. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
3. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
4. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
5. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, w tym:
    a. Brak uprawnień dostępu do informacji,
    b. Informacja tylko do odczytu,
    c. Prawo do edycji informacji,
    d. Brak możliwości wykonania systemowego zrzutu ekranu,
    e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
    f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
    g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.
6. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,

7. Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji,
8. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji,
9. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
10. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

1.3.5. CIS Suite Datacenter Core ALng SA 2L

Prawo do aktualizacji licencji.

Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na wykorzystanie tej licencji w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Ochrona firmware przed atakami poprzez izolację hypervisora technologią Dynamic Root of Trust of Measurement (DRTM).
7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
8. 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 (ACL).
9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

10. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
11. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
13. Możliwość wykorzystania standardu http/2.
14. Wbudowana obsługa TLS 1.3 włączona jako ustawienie standardowe..
15. Możliwość przechowywania wrażliwych danych i kluczy pod ochroną TPM 2.0.
16. Izolacja kernela od pozostałych komponentów systemu w oparciu zabezpieczenia bazujące na wirtualizacji (VBS) chroniąca przed metodami ataków wykorzystujących podatności używane przy „kopaniu" kryptowalut.
17. Dostępność usługi DNS-over-HTTPS (DoH) szyfrujących zapytania DNS przy użyciu HTTPS.
18. Dostępność usługi Server Message Block (SMB) z szyfrowaniem AES-256 (AES-256-GCM and AES-256-CCM), automatycznie wykorzystywanych przy połączeniach z urządzeniami wspierającymi te metody.
19. Szyfrowanie komunikacji i wspólnych zasobów wewnątrz klastra niezawodnościowego.
20. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
21. Wsparcie dla technologii Azure Arc pozwalające na traktowanie serwera zainstalowanego we własnym centrum przetwarzania jako zarządzalnego zasobu Azure.
22. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
23. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
24. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
25. 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),
    d. PIN zdefiniowany dla urządzenia,
    e. Rozpoznawanie twarzy.
26. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
27. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
28. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

29. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
30. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
31. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
32. 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:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. 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 (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,
        iii. 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 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 failover z jednoczesnym zachowaniem pozostałej funkcjonalności.

q. Mechanizmy wirtualizacji mające wsparcie dla:

    i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

    ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

    iii. Obsługi 4-KB sektorów dysków

    iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

    v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

    vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

    vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

33. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
34. Wsparcie dla rozwiązania dla rozwiązań kontenerowych dla aplikacji zgodnych z Kubernetes…
35. Możliwość wykorzystywania aplikacji kontenerowych wymagających wykorzystania Azure Active Directory bez dołączania hosta kontenerów do domeny.
36. Wsparcie migracji zasobów na dyskach do Azure.
37. 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.
38. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
39. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
40. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
41. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
42. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
43. Mechanizm konfiguracji połączenia VPN do platformy Azure.

44. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
45. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
46. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Elementy zarządzania

Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

1. Moduł monitorowania stanu, wydajności i wykorzystania infrastruktury, aplikacji I procesów.
2. Moduł automatyzacji wykonywania zadań w centrum przetwarzania, pozwalający w prosty sposób wykorzystać, łączyć i automatyzować wykonanie natywnych skryptów PowerShell.
3. Moduł powoływania maszyn wirtualnych na platformie Windows Server I zarządzania nimi w ramach centrum przetwarzania, umożliwiający zarządzanie wykorzystania sieci, przestrzeni dyskowych, przetwarzania i uprawnionego dostępu.
4. Moduł ochrony danych poprzez ich bezpieczne składowanie (backup), zarządzanie składowanymi danymi, odtwarzanie danych produkcyjnych. Ma umożliwiać wykorzystanie dla chmury prywatnej, maszyn fizycznych, urządzeń klienckich I aplikacji serwerowych.
5. Moduł wsparcia technicznego dla rozwiązywania problemów technicznych, zarządzania zmianą konfiguracji i zarządzanie cyklem życia serwerów.
6. Moduł zarządzania serwerami I komputerami klasy PC w środowisku własnej organizacji, pozwalający na wykonywanie aktualizacji oprogramowania i zarządzanie aktualizacjami, planowanie i wdrażanie polityk konfiguracyjnych i bezpieczeństwa oraz monitorujący status systemów.
7. Moduł ochrony systemów Windows Server przed złośliwym oprogramowaniem.
8. Integracja umożliwiająca przekazywanie alertów z monitoringu do kanału Microsoft Teams.
9. Możliwość oparcia dostępu do narzędzi w oparciu o rolę administratora w organizacji.
10. Wsparcie dla zarządzania hostami Azure Stack HCI 21H2 i VMware 7.0.

1.3.6. CIS Suite Standard Core ALng SA 2L

Prawo do aktualizacji licencji.

1.3.7. SQLSvrStdCore ALNG SA MVL 2Lic CoreLic

Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym jednego serwera i dwóch wirtualnych środowisk serwerowego systemu operacyjnego.

Serwerowy system operacyjny typ I musi posiadać następujące, wbudowane cechy.

2. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.

3. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
4. Możliwość budowania klastrów składających się z 64 węzłów.
5. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
8. 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 (ACL).
9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
10. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
11. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
13. Możliwość wykorzystania standardu http/2.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. 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),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci,

centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.

20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Ochrona firmware przed atakami poprzez izolację hypervisora technologią Dynamic Root of Trust of Measurement (DRTM).
23. Możliwość przechowywania wrażliwych danych i kluczy pod ochroną TPM 2.0
24. Izolacja kernela od pozostałych komponentów systemu w oparciu zabezpieczenia bazujące na wirtualizacji (VBS) chroniąca przed metodami ataków wykorzystujących podatności używane przy „kopaniu" kryptowalut.
25. Wbudowana obsługa TLS 1.3 włączona jako ustawienie standardowe..
26. Dostępność usługi DNS-over-HTTPS (DoH) szyfrujących zapytania DNS przy użyciu HTTPS.
27. Dostępność usługi Server Message Block (SMB) z szyfrowaniem AES-256 (AES-256-GCM and AES-256-CCM), automatycznie wykorzystywanych przy połączeniach z urządzeniami wspierającymi te metody.
28. Szyfrowanie komunikacji i wspólnych zasobów wewnątrz klastra niezawodnościowego.
29. Wsparcie dla technologii Azure Arc pozwalające na traktowanie serwera zainstalowanego we własnym centrum przetwarzania jako zarządzalnego zasobu Azure.
30. Możliwość wykorzystywania aplikacji kontenerowych wymagających wykorzystania Azure Active Directory bez dołączania hosta kontenerów do domeny.
31. Wsparcie migracji zasobów na dyskach do Azure.
32. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
33. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
34. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
35. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    r. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    s. 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:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

t. Zdalna dystrybucja oprogramowania na stacje robocze.

u. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.

v. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

i. Dystrybucję certyfikatów poprzez http

ii. Konsolidację CA dla wielu lasów domeny,

iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

w. Szyfrowanie plików i folderów.

x. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

y. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.

z. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

aa. Serwis udostępniania stron WWW.

bb. Wsparcie dla protokołu IP w wersji 6 (IPv6),

cc. Wsparcie dla algorytmów Suite B (RFC 4869),

dd. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

ee. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.

ff. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

gg. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.

hh. Mechanizmy wirtualizacji mające wsparcie dla:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

iii. Obsługi 4-KB sektorów dysków

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

36. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
37. Wsparcie dla rozwiązania Kubernetes.
38. 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.
39. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
40. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
41. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
42. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
43. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
44. Mechanizm konfiguracji połączenia VPN do platformy Azure.
45. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
46. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
47. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Elementy zarządzania

Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

11. Moduł monitorowania stanu, wydajności i wykorzystania infrastruktury, aplikacji I procesów.
12. Moduł automatyzacji wykonywania zadań w centrum przetwarzania, pozwalający w prosty sposób wykorzystać, łączyć i automatyzować wykonanie natywnych skryptów PowerShell.
13. Moduł powoływania maszyn wirtualnych na platformie Windows Server I zarządzania nimi w ramach centrum przetwarzania, umożliwiający zarządzanie wykorzystania sieci, przestrzeni dyskowych, przetwarzania i uprawnionego dostępu.
14. Moduł ochrony danych poprzez ich bezpieczne składowanie (backup), zarządzanie składowanymi danymi, odtwarzanie danych produkcyjnych. Ma umożliwiać wykorzystanie dla chmury prywatnej, maszyn fizycznych, urządzeń klienckich I aplikacji serwerowych.
15. Moduł wsparcia technicznego dla rozwiązywania problemów technicznych, zarządzania zmianą konfiguracji i zarządzanie cyklem życia serwerów.
16. Moduł zarządzania serwerami I komputerami klasy PC w środowisku własnej organizacji, pozwalający na wykonywanie aktualizacji oprogramowania i zarządzanie aktualizacjami, planowanie i wdrażanie polityk konfiguracyjnych i bezpieczeństwa oraz monitorujący status systemów.
17. Moduł ochrony systemów Windows Server przed złośliwym oprogramowaniem.

18. Integracja umożliwiająca przekazywanie alertów z monitoringu do kanału Microsoft Teams.
19. Możliwość oparcia dostępu do narzędzi w oparciu o rolę administratora w organizacji.
20. Wsparcie dla zarządzania hostami Azure Stack HCI 21H2 i VMware 7.0.

1.3.8. Azure Prepayment

Miesięczny pakiet subskrypcji standardowej, powszechnie dostępnej przez Internet, typu COTS (Commercial Of-The-Shelf) udostępniający skalowalną platformę i pozwalający wykorzystać w ramach zakupionej puli zasobów – maszyny wirtualne, systemy operacyjne, silniki baz danych, inne aplikacje i usługi PaaS oraz IaaS, spełniający poniżej opisane wymagania.

Pula zasobów zakupionych w pakiecie musi umożliwić wykorzystanie:

a. Minimum 1 jednostka obliczeniowej o parametrach - 1 rdzeń procesora, 1,7 GB RAM, pod kontrolą systemu operacyjnego Windows Server lub Linux (wybrane dystrybucje),
b. Minimum 50 GB dostępnej lokalnie redundantnej przestrzeni dyskowej,
c. Minimum 50 GB dostępnej georedundantnej przestrzeni dyskowej (odległości min. 100km między lokalizacjami),
d. Minimum 100 GB transferu danych do i z usługi miesięcznie.

1. Dostępny portal administracyjny, pozwalający na uruchamianie poprzez wybór dostępnych usług.
2. Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci, systemy operacyjne).
3. Możliwość wyboru różnych rodzajów dysków i ich pojemności.
4. Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów, z możliwością zdalnego dostępu.
5. Komunikacja z mechanizmami zarządzania usługi poprzez REST API.
6. Możliwość przechowywania danych spełniająca następujące wymagania (opcjonalnie dostępnych w ramach usługi):
    a. Wysoka skalowalność, auto-partycjonowanie, load-balancing
    b. Obsługa przechowywania danych udostępnianych jako blob, tablica, dysk, plik, kolejka
    c. Wsparcie dla systemów klienckich Windows i Linux
    d. Skalowalność pojedynczego zasobu pamięci 500TB
    e. Replikacja danych - min. 3 kopie w ramach pojedynczej lokalizacji
    f. Replikacja do innej lokalizacji oddalonej o min 100km od lokalizacji podstawowej
    g. Udostępnienie zasobów pamięci poprzez REST API
    h. Gotowe biblioteki programistyczne środowisk programowania: .NET, Java/Android, Node.js, PHP, Ruby, Python, PowerShell

7. Konfigurowalne usługi wyszukiwania treści w zasobach własnych i internet.
8. Konfigurowalne usługi analizy wyszukanych treści.
9. Dostępność usług umożliwiających uruchamianie aplikacji WWW w modelu gotowej do wykorzystania usługi, z utrzymywanymi przez dostawcę usług komponentami infrastruktury i możliwości w pełni automatycznego skalowania. Usługi te powinny zapewniać możliwość uruchamiania aplikacji działających w minimum następujących technologiach: ASP .NET, PHP, Python, Java, Node,js.
10. Dostępność gotowej usługi realizującej backup serwerów oraz stacji roboczych – zarówno wirtualnych, jak i fizycznych. Usługa musi zapewniać całościowy scenariusz backupu, bez konieczności instalacji komponentów spoza samej usługi, z możliwością definiowania polityk backupowych, wbudowanym szyfrowaniem i możliwością zdefiniowania rozporoszonej geograficznie przestrzeni magazynowej.
11. Dostępność relacyjnej i nierelacyjnej bazy danych, w tym oparte o technologię Hadoop, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
12. Dostępność mechanizmów zarządzania danymi z różnych środowisk wraz z ich klasyfikacją i określeniem uprawnień dostępu.
13. Dostępność mechanizmów integracji danych zawierających::
    a. Mechanizmy zarządzania integracji danych wraz z konektorami do źródeł danych:
        - Dane strukturalne i niestrukturalne,
        - Data Lake,
        - Relacyjne bazy danych,
        - Strumienie danych
    b. Zarządzanie API w postaci hybrydowej, wielochmurowej platformy zarządzania interfejsami API w wybranych środowiskach,
    c. Usługi API dla danych medycznych oparte o rozpowszechnione otwarte standardy,
    d. Usługi umożliwiające tworzenie aplikacji z architekturą opartą na zdarzeniach, z wbudowaną obsługą zdarzeń pochodzących z usług platformy, takich jak obiekty blob magazynu i grupy zasobów.
    e. Usługi tworzenia i uruchamiania zautomatyzowanych przepływów pracy, które integrują aplikacje, dane, usługi i systemy, pozwalające na tworzenie skalowalnych rozwiązań integracyjnych dla scenariuszy A2A i B2B pozwalając łączyć systemy w środowiskach chmurowych, lokalnych i hybrydowych.
    f. Zarządzany broker komunikatów z kolejkami komunikatów oraz tematami publikowania i subskrybowania (w przestrzeni nazw), umożliwiający oddzielanie aplikacji i usług od siebie i zapewniający:
        i. Równoważenie obciążenia między zadaniami,
        ii. Bezpieczne kierowanie i przesyłanie danych oraz kontrolę między granicami usług i aplikacji,
        iii. Koordynowanie prac transakcyjnych, które wymagają wysokiego stopnia niezawodności.
14. Dostępność narzędzi kompleksowego zarządzania danymi w środowiskach hybrydowych.

15. Dostępność środowisk zapewniających możliwość strumieniowego przetwarzania danych z użyciem klastrów opartych o technologie Apache Kafka i Apache Storm dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
16. Możliwość serializacji do określonego formatu tekstowego (np. opartego o XML lub JSON) rozwiązań opartych o maszyny wirtualne, wraz z ich konfiguracją, w sposób umożliwiający ich automatyczną deserializację i utworzenie na tej podstawie gotowego do pracy środowiska.
17. Dostępny portal administracyjny, pozwalający na uruchamianie usług poprzez wybór spośród dostępnych usług.
18. Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci).
19. Włączenie reguł wymuszających stosowanie się do odpowiedniej nomenklatury nazewnictwa zasobów w obrębie środowiska, wymuszając wykorzystanie ustalonego modelu nazw, prefiksów dla określonych typów zasobów
20. Dostępność usług umożliwiających utworzenie prywatnego repozytorium obrazów kontenerów w standardzie zgodnym z Docker.
21. Dostępność usług umożliwiających utworzenie gotowej do działania infrastruktury utrzymania aplikacji w formie kontenerów zgodnych z Docker – usługi działającej w formie PaaS, w szczególności bez konieczności ręcznego konfigurowania węzłów roboczych i zarządzających
22. Dostępność relacyjnych baz danych, zgodnych z MySQL i z PostgreSQL, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
23. Dostępność bazy danych typu NoSQL, oferującej API dostępowe zgodne z MongoDB dostępnej jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
24. Przynajmniej dwa jasno zdefiniowane poziomy spójności danych dla bazy NoSQL.
25. Możliwość automatycznej dystrybucji danych pomiędzy różne regiony oraz ulokowane w nich centra obliczeniowe wraz z możliwością ręcznego jak i automatycznego przełączania replik
26. Możliwość zestawienia dedykowanego łącza pomiędzy siedzibą Zamawiającego a dostawcą usług chmurowych w technologii opartej o światłowody.
27. Posiadanie przez dostawce centrów przetwarzania, działających w trybie 24/7 zespołów monitorujących i zwalczających cyberataki oraz przedstawiających cykliczne raporty na temat aktualnych zagrożeń i sposobie ich zwalczania.
28. Akcelerowana, definiowana programowo sieć wirtualna w środowisku, wspierająca akceleracje SR-IOV, realizowana na akcelerowanych interfejsach sieciowych FPGA, do 30Gb/s.
29. Możliwość śledzenia ruchu sieciowego
30. Dostępność mechanizmów analizy działania wielowarstwowych aplikacji poprzez umieszczanie kodu JavaScript wewnątrz stron internetowych lub doklejanie kodu do aplikacji czy instalacji agenta na serwerze umożliwiając korelowanie i analizowanie od frontu po sam serwer aplikacji czy bazy danych
31. Możliwość wykorzystania usług SMB 3.0 do współdzielenia plików wykorzystując szyfrowanie podczas transmisji, jako usługa
32. Możliwość zdefiniowania szablonu maszyny wirtualnej włącznie z konfiguracją aplikacji, uruchamiania serwisów poprzez zdefiniowanie stanu oczekiwanego w postaci plików konfiguracyjnych.

33. Możliwość budowania potoków automatyzacji wdrażania i uruchamiania aplikacji zarówno w postaci infrastruktury pod aplikację, jak i budowania kontenerów oraz wdrażania i uruchamiania aplikacji, testowania aplikacji i generowania raportów z procesu

Przewidywalny koszt budowy i utrzymania

1. Oparcie się o usługi typu subskrypcji standardowej, powszechnie dostępnej przez internet usługi hostowanej typu COTS (Commercial Of-The-Shelf) o przewidywalnym koszcie określonym jasnymi zasadami wyceny.
2. Dostępność kalkulatora wykorzystania usługi pozwalającego na oszacowanie kosztów wykorzystania zakupionej puli zasobów.
3. Możliwość zmiany wymaganych parametrów usługi i jej skalowania zgodnie z potrzebami.
4. Możliwość automatycznego skalowania mocy obliczeniowej usług.
5. Płatność za fizyczne wykorzystanie usług z możliwością ich okresowego wyłączania.

Zgodność ze standardami

1. Dostępność narzędzi wspomagających migrację aplikacji i danych zarówno ze środowisk własnych do usługi, jak i z usługi na dowolną inną platformę opartą o standard serwerów x64, a więc pozwalających na przeniesienie usług w przypadku podjęcia takiej decyzji.
2. Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy, potwierdzonych aktualnymi wynikami audytów, w szczególności:

- ISO 27001, ISO 27002, ISO 27017, ISO 27018
- SOC 1, SOC 2, SOC 3
- Open Authentication Standard – OAuth

W zakresie interoperacyjności:

- HTTP(S) - TLS
- Docker
- REST API

W zakresie programowania:

- Java
- .NET
- PHP
- Python
- Node.js
- Wsparcie narzędziowe w Visual Studio i Eclipse

3. Wsparcie usługi dla standardowych rozwiązań OpenSource takich jak WordPress, Joomla, Drupal, OrchardCMS, MediaWiki, phpBB. Dostępność w ramach usługi predefiniowanych obrazów z tym oprogramowaniem.

Dostępność systemów i ich bezpieczeństwo

1. Zgodność z EU Cloud Code of Conduct potwierdzona na stronie eucoc.cloud.
2. Usługa powinna zapewniać SLA na wszystkie swoje usługi (łącznie z pojedynczą instancją maszyny wirtualnej) na poziomie minimum 99,9%.

3. Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach.
4. 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.
5. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi.
6. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
7. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi.
8. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
9. Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
10. 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".
11. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych.
12. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN)
13. Wbudowane mechanizmy zabezpieczające przez atakami DDoS.
14. Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 500 km, znajdujące się na terenie Unii Europejskie.j
15. Silnik rekomendacji zabezpieczeń infrastruktury oparty o algorytmy nauczania maszynowego.
16. Dostępność usługi umożliwiającej przechowywanie certyfikatów, haseł dostępu zgodnie ze standardem FIPS 140-2 poziomu 2.
17. Gradacja zakresu uprawnień i budowa konfigurowalnych zasad i ról dostępu do środowiska do poziomu pojedynczych kart sieciowych, dysków czy zarządzania uprawnieniami (tzw. RBAC, Role-Based Access Control).
18. Dostępność usługi katalogu tożsamości i przynależności użytkowników do grup wspierający OAuth2 oraz pojedynczego logowania, umożliwiający budowanie logowania przy pomocy dostawców firm trzecich.
19. Oba centra danych powinny posiadać przynajmniej trzy z wymienionych certyfikacji: TIER-III, UK G-Cloud, ENISA IAF, SOC 1, SOC 2.
20. Zamawiający wymaga dostępności następujących mechanizmów bezpieczeństwa w ramach usługi:
    - Bramki VPN.
    - Obsługi IPSec.
    - Akceleracji SSL.
    - Firewalla warstwy aplikacyjnej – WAF
    - Load balancera wspierającego Cookie Affinity

- Systemu przeciwdziałania włamaniom – IPS.
- Systemu wykrywania włamań - IDS.
- Zasoby ludzkie w zakresie utrzymania usługi realizacji zadania prewencji, identyfikacji zagrożeń oraz natychmiastowe reagowanie na wszelkie incydenty bezpieczeństwa IT.

21. Posiadanie przez dostawce centrów przetwarzania, działających w trybie 24/7 zespołów monitorujących i zwalczających cyberataki oraz przedstawiających cykliczne raporty na temat aktualnych zagrożeń i sposobie ich zwalczania.

Zgodność z obowiązującym prawem Polskim i Unijnym

1. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych.
2. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów członkowskich Unii Europejskiej.
3. Zobowiązania umowne potwierdzające zgodność z RODO.
4. Zapewnienie przetwarzania danych osobowych zgodnie z wymaganiami przepisów prawa a w szczególności w zakresie ochrony danych osobowych w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).
5. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego.
6. Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.
7. Gwarancja usunięcia danych Zamawiającego z usługi po zakończeniu umowy.
8. Gwarancja braku dostępu do danych Zamawiającego w usłudze, z wyłączeniem działań serwisowych wykonywanych wyłącznie przez uprawnione osoby z organizacji Dostawcy usługi.
9. Gwarancja usunięcia danych w terminie do 120 dni od wygaśnięcia subskrypcji i zakończenia umowy.