numer sprawy: OR-AG-I.ZP.D.272.61.2022.AS
załącznik nr 2 do specyfikacji warunków zamówienia (SWZ)

Opis przedmiotu zamówienia

Spis treści

1 ROZDZIAŁ I – Przedmiot zamówienia, informacje ogólne

1. Przedmiotem zamówienia jest dostawa licencji oprogramowania, praw do aktualizacji licencji oprogramowania standardowego oraz dostawa pakietów subskrypcji usług standardowych (Produktów), w tym:
   1) subskrypcja pakietów usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego,
   2) świadczenie usług Software Assureance dla posiadanych licencji oprogramowania Microsoft,
   3) dostawa usług hostowanych Microsoft Azure,
   4) dostawa oprogramowania standardowego.
2. Szczegółowy zakres podmiotowy, przedmiotowy i ilościowy przedmiotu zamówienia został określony w rozdziale II OPZ.
3. Zamawiający informuje, że posiada obecnie umowę Enterprise Agreement o numerze E7370715 oraz Rejestrację o numerze 56568381, której ważność kończy się 30 września 2022 roku.
4. Zamawiający wymaga dostaw licencji oprogramowania przeznaczonych do wykorzystania przez jednostki administracji publicznej.
5. Zamówienie obejmuje dostawę przedmiotu zamówienia dla następujących jednostek:
   a) Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie,
   b) Mazowieckiej Jednostki Wdrażania Programów Unijnych,
   c) Mazowieckiego Zarządu Dróg Wojewódzkich w Warszawie.
6. Wskazane jednostki posiadają niezależne środowiska chmurowe (tenanty) na platformie Microsoft, na których musi być zapewniona kontynuacja subskrypcji oprogramowania Office 365. Nazwy środowisk chmurowych (tenantów) zostały wskazane w Rozdziale II – przy zestawieniu ilościowym dla poszczególnych jednostek.

2 ROZDZIAŁ II – Zakres zamówienia, zestawienie ilościowe

Poniżej wskazano zakres zamówienia w podziale na jednostki, numery katalogowe wymaganych Produktów, ich ilość dla poszczególnych jednostek oraz wskazanie opisu równoważności w dalszej części dokumentacji. Zamawiający podkreśla, że poszczególne jednostki posiadają niezależne środowiska chmurowe (tenanty) na platformie Microsoft, na których musi być zapewniona kontynuacja subskrypcji oprogramowania Microsoft Office 365. Przy poszczególnych tabelach umieszczone zostały nazwy środowisk chmurowych (tenantów).

Tabela 1 - Specyfikacja ilościowa przedmiotu zamówienia UMWM (Urząd Marszałkowski Województwa Mazowieckiego w Warszawie)

Tenant: mazovia.onmicrosoft.com (8C1D62E4)

LP.	Nazwa produktu	Numer katalogowy	Ilość	Opis równoważności
1	M365 E3 Unified FSA Sub Per User	AAD-33200	1221	rozdz.V pkt 5.1
2	M365 E3 Unified Sub Per User	AAD-33204	209	rozdz.V pkt 5.1
3	O365 E1 Sub Per User	T6A-00024	50	rozdz.V pkt 5.2
4	CIS Suite Standard Core ALng SA 2L	9GA-00313	88	rozdz.V pkt 5.3
5	CIS Suite Datacenter Core ALng SA 2L	9GS-00135	40	rozdz.V pkt 5.4
6	SQL Server Standard Core ALng SA 2L	7NQ-00292	10	rozdz.V pkt 5.5
7	SQL Server Enterprise Core ALng SA 2L	7JQ-00343	4	rozdz.V pkt 5.6
8	Win Remote Desktop Services CAL ALng SA UCAL	6VC-01254	150	rozdz.V pkt 5.7
9	Win Server External Connector ALng SA	R39-00396	3	rozdz.V pkt 5.8
10	Azure prepayment	6QK-00001	5	rozdz.V pkt 5.9
11	Win Server DC Core ALng SA 2L	9EA-00278	16	rozdz.V pkt 5.10

Tabela 2 - Specyfikacja ilościowa przedmiotu zamówienia MJWPU (Mazowiecka Jednostka Wdrażania Programów Unijnych)

Tenant: mjwpu365.onmicrosoft.com (88B04B67)

LP.	Nazwa produktu	Numer katalogowy	Ilość	Opis równoważności
1	M365 E3 Unified FSA Sub Per User	AAD-33200	520	rozdz.V pkt 5.1
2	CIS Suite Datacenter Core ALng SA 2L	9GS-00135	64	rozdz.V pkt 5.4
3	SQL Server Standard Core ALng SA 2L	7NQ-00292	6	rozdz.V pkt 5.5
4	Win Server External Connector ALng SA	R39-00396	3	rozdz.V pkt 5.8
5	SQL Server Standard Core ALng LSA 2L	7NQ-00302	14	rozdz.V pkt 5.5
6	Defender O365 P2 Sub Per User	FSZ-00002	20	rozdz.V pkt 5.11
7	Defender Endpoint P2 Sub Per User	QLS-00003	20	rozdz.V pkt 5.12
8	System Center DC Core ALng LSA 2L	9EP-00037	2	rozdz.V pkt 5.13
9	Power BI Pro Sub Per User	NK4-00002	10	rozdz.V pkt 5.14

Tabela 3 - Specyfikacja ilościowa przedmiotu zamówienia MZDW (Mazowiecki Zarząd Dróg Wojewódzkich w Warszawie)

Tenant: mzdw.onmicrosoft.com (9012901B)

LP.	Nazwa produktu	Numer katalogowy	Ilość	Opis równoważności
1	M365 E3 Unified Sub Per User	AAD-33204	265	rozdz.V pkt 5.1
2	Win Server Standard Core ALng SA 2L	9EM-00270	130	rozdz.V pkt 5.15
3	SQL Server Standard Core ALng SA 2L	7NQ-00292	4	rozdz.V pkt 5.5
4	Project P3 Sub Per User	7LS-00002	1	rozdz.V pkt 5.16
5	Win Server Standard Core ALng LSA 2L	9EM-00562	8	rozdz.V pkt 5.15

3 ROZDZIAŁ III – Minimalne wymagania w zakresie dostaw

1. Oferowane Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).
2. Licencje na oprogramowanie muszą zawierać prawo w okresie trwania umowy EA do uaktualniania wersji zakupionego oprogramowania będącego przedmiotem zamówienia do najbardziej aktualnej dostępnej wersji.
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, nie gorszych niż opisanych w OPZ oraz zasad ich używania wraz ze zobowiązaniami Dostawcy w zakresie ochrony danych.
7. Z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga oferty zawierającej Produkty pochodzące od jednego Producenta (producenta produktów lub jego spółek zależnych), umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego.
8. Zamawiający dopuszcza składanie ofert na Produkty o szerszej niż wymagana funkcjonalności lub Produkty następcze.
9. Dla oprogramowania z licencjami wieczystymi wymagane jest zapewnienie możliwości korzystania z kopii zamiennych (możliwość instalacji oprogramowania na wielu urządzeniach przy wykorzystaniu jednego standardowego obrazu), z prawem do:

a) wielokrotnego użycia jednego obrazu dysku w procesie instalacji,

b) tworzenia kopii zapasowych

c) masowej aktywacji oprogramowania przy użyciu jednego klucza aktywacyjnego dla danego typu oprogramowania.

10. Wykonawca zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym osobom ze strony Zamawiającego na:

d) Pobieranie zakupionego oprogramowania,

e) Aktywację pakietów subskrypcji,

f) Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania,

g) Sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów.

11. Zamawiający wymaga udzielenia uprawnień na stronie producenta oraz dostępu do wersji instalacyjnych zamawianego oprogramowania i kluczy licencyjnych w terminie do 5 dnia roboczego następnego miesiąca po podpisaniu umowy.
12. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym.
13. Jeżeli nowa (następcza) 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.
14. 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.
15. Zgodność algorytmów zabezpieczających dane usług platformy hostowanej Dostawcy z FIPS 140.
16. 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.

4 ROZDZIAŁ IV – Rozwiązania równoważne

Zamawiający dopuszcza możliwość zaoferowania Produktów Równoważnych. W rozdziale V oraz w poniższej części przedstawione są wymagania i kryteria równoważności w przypadku zaoferowania Produktów Równoważnych:

a) Zamawiający wymaga, aby oferowane Produkty Równoważne spełniały wymagania określone w rozdziale V. odpowiednio dla każdego Produktu równoważnego oraz niżej wymienione wymagania. Produkt Równoważny musi bez zakłóceń współpracować z posiadaną przez Zamawiającego infrastrukturą sprzętową oraz wykorzystywanym oprogramowaniem i systemami, do których należą: serwery, laptopy, komputery stacjonarne, urządzenia drukujące i skanujące, urządzenia sieciowe, oprogramowanie systemowe Microsoft Windows, Windows Server, oprogramowanie Microsoft SharePoint i Project Server, środowisko wirtualizacyjne HyperV oraz VmWare. Na Wykonawcy oferującym Produkty równoważne spoczywa odpowiedzialność w zakresie prawidłowego działania zaoferowanych Produktów w środowisku pracy użytkowników Produktów po stronie Zamawiającego;
b) Wykonawca musi zapewnić warunki i zakres usługi Wsparcia Technicznego Producenta dla Produktów równoważnych nie gorsze niż usługa określona dla odpowiedniego Produktu Producenta Microsoft;
c) Wykonawca musi wykazać, że funkcjonalność każdego Produktu równoważnego nie jest gorsza od funkcjonalności odpowiedniego Produktu Producenta Microsoft;

d) Wykonawca musi zapewnić, że Produkty równoważne są kompatybilne i będą w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem systemowym, aplikacyjnym i użytkowym, eksploatowanym i obsługiwanym przez Zamawiającego;
e) Wykonawca zobowiązany jest przeszkolić pracowników Zamawiającego w zakresie funkcjonalności i działania Produktów równoważnych w terminie ustalonym z Zamawiającym, lecz nie później niż w okresie 30 dni kalendarzowych od daty zawarcia Umowy;
f) Wykonawca zobowiązany jest pokryć koszty zmiany w zakresie Produktów Microsoft na Produkty i rozwiązania Równoważne, konieczne do właściwego działania środowiska sprzętowo-programowego Zamawiającego, o ile wystąpi taka konieczność;
g) Wykonawca zobowiązany jest przywrócić sprawne działanie infrastruktury sprzętowo-
h) programowej Zamawiającego oraz na własny koszt dokonać niezbędnych modyfikacji przywracających właściwe działanie tego środowiska sprzętowo-programowego, również po odinstalowaniu Produktu równoważnego w przypadku, gdy zaoferowane Produkty równoważne nie będą właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy tego środowiska sprzętowo-programowego,

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:

17. 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 (Produktu). W odniesieniu do oprogramowania mogą zostać dostarczone licencje lub subskrypcje tymczasowe, w pełni zgodne z oferowanymi.
18. 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
19. Negatywny wynik sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 226 ust. 1 pkt. 5 Pzp – z powodu niezgodności treści oferty z warunkami zamówienia.
20. 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.
21. Po przeprowadzeniu weryfikacji, dostarczone do testów produkty zostaną zwrócone wykonawcy.
22. Zamawiający zastrzega sobie także możliwość odwołania się w trakcie procesu weryfikacji równoważności do oficjalnych, publicznie dostępnych stron internetowych producenta weryfikowanego przedmiotu oferty.

5 ROZDZIAŁ V – Informacje dotyczące Produktów Równoważnych - warunki równoważności produktów

5.1 M365 E3 Unified FSA Sub Per User oraz M365 E3 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:
15. Monitorowanie zabezpieczeń pakietu, aplikacji i urządzeń,
16. Raportowanie bieżącego stanu zabezpieczeń organizacji,
17. Poprawianie stanu bezpieczeństwa dzięki możliwości odnajdowania komponentów źle zabezpieczonych,
18. Porównanie wskaźników bezpieczeństwa z wzorcami i ustalanie kluczowych wskaźników dla bezpieczeństwa (KPI).

5.2 O365 E1 Sub Per User

Pakiet subskrypcji standardowych usług hostowanych (on-line) typu COTS (Commercial Of-The-Shelf) ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line – usługi zarządzania tożsamością użytkowników, portalu wewnętrznego, poczty elektronicznej, narzędzi wiadomości błyskawicznych, konferencji głosowych i video, repozytorium dokumentów, wewnętrznego serwisu społecznościowego oraz edycji dokumentów biurowych on-line (dalej Usługi).

Wymagania dotyczące pakietu subskrypcji usługi Dostawcy Usług Cyfrowych:

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.

Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.

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.

Wbudowana usługa zarządzania tożsamością użytkowników musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.

Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.

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”.

Gwarantowana dostępność usług platformy na poziomie 99,9%,

Możliwość dodawania do 500 własnych nazw domenowych.

Dostępność portalu administracyjnego do zarządzania usługą oraz zasadami grup.

Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.

Ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day.

Szyfrowanie danych przesyłanych za pomocą sieci publicznych.

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.

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.

Dostępność raportów zgodności z WCAG.

Dostępność raportów zgodności z EN 301 549.

Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy.

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

Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,

Wbudowane mechanizmy zabezpieczające przez atakami DDoS,

Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km.

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.

Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.

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.

Zobowiązania umowne potwierdzające zgodność z rozp. RODO i potwierdzające rolę operatora usługi jako przetwarzającego dane,

Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,

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. zarządzania zasobami

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),
- Urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 40 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 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

Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania

Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań

Obsługa list i grup dystrybucyjnych.

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

Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co 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.

Dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów – z poziomu urządzeń mobilnych.

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

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.

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 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.

Usługa portali on-line muszi 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

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

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. 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

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 2019.

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

7. Bezpieczną komunikację głosową oraz video,
8. Przesyłanie wiadomości błyskawicznych (tekstowych),
9. Możliwość organizowania telekonferencji,
10. Możliwość przesyłania strumieniowego prezentacji video i głosowej,
11. 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 zapraszania do spotkań zdalnych użytkowników zewnętrznych nieposiadających licencji usługi.
21. Możliwość oceny jakości komunikacji głosowej i wideo.
22. Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze.
23. 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.
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 stworzenia poczekalni dla dołączających użytkowników z dołączaniem ich decyzją uprawnionych osób.
27. Możliwość zastąpienia tła lub jego rozmycia w przypadku transmisji video.
28. 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.
29. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.
30. Możliwość (w przypadku nabycia odpowiednich licencji) realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
31. Możliwość nagrywania telekonferencji przez uczestników z zapisem nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
32. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.

33. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
34. 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,
    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 UKW.

Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 1 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.

5.3 CIS Suite Standard Core ALng SA 2L

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.

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. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
7. 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).
8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
9. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
10. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
11. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
12. Możliwość wykorzystania standardu http/2.
13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
17. 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),
18. 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.
19. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
20. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
21. Ochrona firmware przed atakami poprzez izolację hypervisora technologią Dynamic Root of Trust of Measurement (DRTM).
22. Możliwość przechowywania wrażliwych danych i kluczy pod ochroną TPM 2.0
23. Izolacja kernela od pozostałych komponentów systemu w oparciu zabezpieczenia bazujące na wirtualizacji (VBS) chroniąca przed metodami ataków wykorzystujących podatności używane przy „kopaniu” kryptowalut.
24. Wbudowana obsługa TLS 1.3 włączona jako ustawienie standardowe..
25. Dostępność usługi DNS-over-HTTPS (DoH) szyfrujących zapytania DNS przy użyciu HTTPS.

26. 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.
27. Szyfrowanie komunikacji i wspólnych zasobów wewnątrz klastra niezawodnościowego.
28. Wsparcie dla technologii Azure Arc pozwalające na traktowanie serwera zainstalowanego we własnym centrum przetwarzania jako zarządzalnego zasobu Azure.
29. Możliwość wykorzystywania aplikacji kontenerowych wymagających wykorzystania Azure Active Directory bez dołączania hosta kontenerów do domeny.
30. Wsparcie migracji zasobów na dyskach do Azure.
31. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
32. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
33. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
34. 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.

35. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
36. Wsparcie dla rozwiązania Kubernetes.
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.

5.4 CIS Suite Datacenter Core ALng SA 2L

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:
    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.

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:

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.

5.5 SQL Server Standard Core ALng SA 2L

System bazodanowy (SBD) licencjonowany na rdzenie procesora musi spełniać następujące wymagania poprzez wbudowane mechanizmy:

1. Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
5. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
6. SBD musi umożliwiać tworzenie klastrów niezawodnościowych.
7. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:
   - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
   - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
   - klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
8. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
9. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.
10. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł

użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.

11. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.

12. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń:

    - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),
    - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),
    - para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).

13. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.

14. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków" obiektu, „rodzica" itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.

15. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:

    - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
    - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
    - udostępniać język zapytań do struktur XML,
    - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
    - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.

16. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:

    - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
    - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
    - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
    - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).

17. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania.

18. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożliwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.

19. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.

20. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.

21. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.

22. System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:

    - mechanizm debuggowania tworzonego rozwiązania,
    - mechanizm stawiania „pułapek” (breakpoints),
    - mechanizm logowania do pliku wykonywanych przez transformację operacji,
    - możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),
    - możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)
    - mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),
    - mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),
    - mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
    - mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych.

23. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.

24. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane

w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).

25. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
26. Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
27. Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
28. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
29. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.
30. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać:
    - raporty parametryzowane,
    - cache raportów (generacja raportów bez dostępu do źródła danych),
    - cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),
    - współdzielenie predefiniowanych zapytań do źródeł danych,
    - wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
    - możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
    - możliwość wizualizacji wskaźników KPI,
    - możliwość wizualizacji danych w postaci obiektów sparkline.
31. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
32. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF, PowerPoint.
33. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.
34. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).
35. Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.

36. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.
37. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.
38. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).
39. SBD musi posiadać wbudowane mechanizmy do obsług danych grafowych (struktur złożonych z węzłów i krawędzi - reprezentujących relacje między węzłami). System musi mieć wbudowane funkcje (dostępne z poziomu kodu SQL) do analizy powiązań między węzłami grafu oraz wyszukiwania najkrótszej ścieżki w grafie.
40. SBD musi posiadać mechanizmy klasyfikacji informacji przechowywanych w bazie danych w celu łatwej identyfikacji obszarów (obiektów) w bazie danych, gdzie składowane są dane wrażliwe. Mechanizm ten powinien umożliwiać przypisanie kolumnom w tabeli m.in. takich atrybutów jak: typ przechowywanych informacji oraz poziom wrażliwości danych. Dodatkowo SBD powinien udostępniać zestaw predefiniowanych raportów prezentujących m.in. listę sklasyfikowanych tabel i kolumn oraz liczbę tabel zawierających dane wrażliwe.

5.6 SQL Server Enterprise Core ALng SA 2L

Serwer relacyjnej bazy danych (SBD) licencjonowany na rdzenie procesora musi spełniać poniższe wymagania poprzez wbudowane mechanizmy:

1. Możliwość wykorzystania SBD, jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
5. Wykonywanie typowych zadań administracyjnych w trybie on-line - SBD musi umożliwiać wykonywanie typowych zadań administracyjnych (indeksowanie, backup, odtwarzanie danych) bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednoużytkownikowy.
6. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
7. Skalowalność systemu - SBD powinien wspierać skalowanie w kontekście wielkości rozwiązania (powinien być dostępny zarówno na platformie wieloserwerowej, jak również średniej wielkości komputerów i urządzeń mobilnych).
8. Możliwość dodawania procesorów bez restartu systemu - SBD powinien umożliwiać dodanie procesora do systemu, bez konieczności restartu silnika bazy danych.

9. Kopie bazy tylko do odczytu - SBD powinien umożliwiać tworzenie w dowolnym momencie kopii bazy danych tylko do odczytu zawierającej stan bazy z bieżącego momentu czasu. Wiele takich kopii może być równolegle użytkowanych w celu wykonywania z nich zapytań.

10. Możliwość dodawania pamięci bez restartu systemu - SBD powinien umożliwiać dodanie pamięci do systemu bez konieczności restartu silnika bazy danych.

11. SBD musi umożliwiać tworzenie klastrów niezawodnościowych. Powinien również umożliwiać tworzenie klastrów niezawodnościowych, których węzły znajdują się w różnych podsieciach komputerowych.

12. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między wieloma lokalizacjami (podstawowa i zapasowe) przy zachowaniu następujących cech:

    - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
    - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
    - duplikacja danych w trybie synchronicznym lub asynchronicznym,
    - SBD musi umożliwiać duplikację danych z ośrodka podstawowego, do co najmniej 8 lokalizacji zapasowych,
    - SBD musi umożliwiać duplikację danych z ośrodka podstawowego, do co najmniej 4 lokalizacji zapasowych w trybie synchronicznym,
    - w celu zwiększenia skalowalności i wydajności systemu SBD musi umożliwiać korzystanie z kopii baz w lokalizacjach zapasowych w trybie tylko do odczytu (raportowanie, tworzenie backupów itp.) bez przerywania działania mechanizmu duplikacji danych z ośrodka podstawowego,
    - klienci bazy danych mogą być automatycznie przełączeni do bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
    - brak limitu odległości między systemami (dopuszczalne są tylko limity w minimalnej wymaganej przepustowości łącza oraz limity wynikające z opóźnień na łączu),
    - kompresja danych przesyłanych między serwerem podstawowym i zapasowym (w celu minimalizacji obciążenie sieci),
    - system automatycznie naprawia błędy pamięci masowej (w przypadku odkrycia błędu fizycznego odczytu danych z pamięci masowej, poprawny fragment danych jest transferowany z drugiego systemu i korygowany).

13. Replikacja danych i modyfikacja w wielu punktach - SBD powinien pozwalać na transakcyjną replikację wybranych danych z bazy danych między wieloma węzłami. Dodanie lub usunięcie węzła nie powinno wpływać na funkcjonowanie i spójność systemu replikacji, ani nie powinno przerywać procesu replikacji. Dane mogą w takim schemacie replikacji być modyfikowane w dowolnym węźle, (ale tylko w jednym węźle w danym momencie). System powinien zawierać narzędzie do nadzorowania i wizualizacji topologii oraz stanu procesu replikacji. Dodatkowo SBD powinien umożliwiać kompresję przesyłanych danych między serwerami uczestniczącymi w replikacji, aby minimalizować obciążenie łączy sieciowych.

14. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.

15. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania powinien wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.

16. Możliwość szyfrowania przechowywanych danych - SBD musi pozwalać na szyfrowanie przechowywanych danych. Szyfrowanie musi być cechą SBD i nie może wymagać jakichkolwiek zmian w aplikacjach korzystających z danych. Zaszyfrowanie lub odszyfrowanie danych nie powinno powodować przerwy w dostępie do danych. Kopia bezpieczeństwa szyfrowanej bazy także powinna być automatycznie zaszyfrowana.

17. Korzystanie z zewnętrznych urządzeń do przechowywania kluczy szyfrujących - SBD powinien posiadać mechanizm pozwalający na przechowywanie kluczy szyfrujących na urządzeniach zewnętrznych (np. czytniki kart). Rozwiązanie to powinno być otwarte, to znaczy pozwalać na dodawanie w przyszłości

obsługi urządzeń nowych, oczywiście pod warunkiem dostarczenia przez producenta urządzenia odpowiednich modułów oprogramowania zgodnych z SBD.

18. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.

19. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.

20. Ograniczenie użycia zasobów – SBD powinien posiadać wbudowany mechanizm ograniczający wykorzystanie zasobów systemu operacyjnego (% wykorzystania czasu procesora, % wykorzystania pamięci, liczba operacji wejścia/wyjścia podsystemu dyskowego). Reguły definiujące ograniczenia dla użytkowników lub grup użytkowników dotyczące wykorzystania zasobów powinny mieć możliwość użycia w nich logiki zaimplementowanej za pomocą języka programowania (np. używanego w danym SBD języka SQL).

21. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.

22. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.

23. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych powinien udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).

24. System SDB musi łączyć w sobie cechy bazy przechowywanej w pamięci RAM (IMDB) oraz tradycyjnej bazy danych (RDBMS) przechowywanej na dyskach.

25. System SDB musi zapewniać w ramach tej samej bazy danych możliwość umieszczenia wybranych tabel w pamięci RAM serwera, a pozostałych tabel w tradycyjnej postaci (na dysku).

26. SBD musi posiadać możliwość korzystania w procedurach jednocześnie z tabel przechowywanych w pamięci RAM oraz tabel przechowywanych na dyskach.

27. System SDB musi zapewniać wersjonowanie wierszy w tabelach przechowywanych w pamięci RAM.

28. W celu zwiększenia wydajności SBD musi posiadać możliwość tworzenia procedur składowanych w kodzie natywnym, to znaczy takich procedur, które są automatycznie kompilowane do kodu natywnego podczas ich tworzenia oraz składają się z instrukcji procesora, które nie wymagają dalszych kompilacji lub interpretacji.

29. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń (rejestrowanie tylko zdarzeń spełniających zdefiniowane warunki filtrujące, np. dotyczących tylko wskazanego obiektu). Wymagana jest rejestracja zdarzeń:

    - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),

    - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),

    - para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).

30. Możliwość rejestrowania bardzo dużej liczby zdarzeń i analizowania ich z minimalnym opóźnieniem – SBD powinien dostarczać wbudowaną platformę do tworzenia aplikacji typu CEP (Complex Event

Processing). Aplikacje takie umożliwiają rejestrowanie bardzo dużej liczby zdarzeń (np. odczytów liczników lub z innych urządzeń pomiarowych, dowolnych zdarzeń występujących z dużą częstotliwością) i reagowanie na nie z minimalnym opóźnieniem. System powinien również udostępniać mechanizmy wysokiej dostępności dla tej usługi.

31. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.

32. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków" obiektu, „rodzica" itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.

33. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:

    - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
    - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
    - udostępniać język zapytań do struktur XML,
    - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
    - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.

34. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:

    - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
    - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
    - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
    - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).

35. Możliwość efektywnego przechowywania dużych obiektów binarnych - SBD powinien umożliwiać przechowywanie i efektywne zarządzanie dużymi obiektami binarnymi (pliki graficzne, multimedialne, dokumenty, itp.). Obiekty te nie powinny być przechowywane w plikach bazy danych, ale w systemie plików. Jednocześnie pliki te powinny być zarządzane przez SBD (kontrola dostępu na podstawie uprawnień nadanych w SBD). Dodatkowo dane binarne powinny być dostępne dla użytkowników bazy danych jako standardowa kolumna tabeli (dostęp z poziomu zapytań języka SQL obsługiwanego przez SBD).

36. Możliwość kompresji przechowywanych danych - SBD powinien udostępniać wbudowany mechanizm kompresji zgromadzonych danych w celu osiągnięcia lepszej wydajności przy niezmienionej konfiguracji sprzętowej. System kompresji powinien umożliwiać również kompresję UNICODE systemem UCS-2.

37. Możliwość rejestracji zmiany w rekordzie danych – SBD powinien pozwalać na rejestrację zmian w danych włącznie z zapamiętaniem stanu pojedynczego rekordu danych sprzed modyfikacji. Rozwiązanie nie powinno ujemnie wpływać na wydajność systemu i powinno być konfigurowalne bez wpływu na istniejące aplikacje korzystające z danych. Rozwiązanie powinno rejestrować także zmiany w definicji struktur danych.

38. Audyt dostępu do danych - SBD powinien pozwalać na rejestrację operacji takich jak: logowanie, wylogowanie użytkownika, zmiany w definicji obiektów bazy danych (tabele, procedury), wykonywanie przez wskazanego użytkownika operacji takich jak SELECT, INSERT, UPDATE, DELETE. Rozwiązanie powinno być niezależne od aplikacji, wbudowane w SBD.

39. Partycjonowanie danych - SBD powinien pozwalać na podział danych w jednej tabeli między różne fizyczne pamięci masowe zgodnie ze zdefiniowanymi warunkami podziału. Powinien udostępniać mechanizm równoległego (wielowątkowego) dostępu do danych umieszczonych w różnych partycjach. Dodatkowo powinna być dostępna możliwość szybkiego przesyłania dużych zbiorów danych poprzez mechanizm przełączania partycji (czyli dane przenoszone są z jednej tabeli do drugiej za pomocą operacji na metadanych, a nie przez fizyczne kopiowanie rekordów). Dzięki takiej funkcjonalności możliwe jest przeniesienie dużej liczby rekordów w bardzo krótkim czasie (rzędu sekund). Dodatkowo minimalizowane jest odczuwanie wpływu tej operacji przez użytkowników (minimalny wpływ przenoszenia danych na obciążenie systemu).

40. Wsparcie dla Indeksów kolumnowych - SBD powinien umożliwiać tworzenie indeksów przechowujących dane osobno dla każdej z kolumn tabeli łącząc je następnie w całość. Indeks powinien również wykorzystywać mechanizm kompresji oraz pozwalać na modyfikowanie danych w tabeli, dla której taki indeks utworzono. Dodatkowo tworzenie indeksu powinno być możliwe w trybie online czyli w trakcie wprowadzania modyfikacji indeksowanych danych.

41. Indeksowanie podzbioru danych w tabeli - SBD powinien umożliwiać tworzenie indeksów na podzbiorze danych z tabeli określonym poprzez wyrażenie filtrujące.

42. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System powinien umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo powinien udostępniać środowisko do debuggowania.

43. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.

44. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.

45. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.

46. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.

47. System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Zestaw standardowych dostępnych transformacji powinien obejmować takie transformacje jak: sortowanie, wyszukiwanie wartości według klucza w tabelach słownikowych, automatyczna obsługa SCD (*Slowly Changing Dimension*) w zasilaniu hurtowni danych, pobranie danych z serwera FTP, wysłanie e-maila, łączenie danych z wykorzystaniem logiki rozmytej, poprawa jakości danych wykorzystująca integrację z dedykowanym systemem zarządzania jakością danych oraz jego bazą wiedzy i reguł walidujących. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:

    - mechanizm debuggowania tworzonego rozwiązania,
    - mechanizm stawiania „pułapek” (breakpoints),
    - mechanizm logowania do pliku wykonywanych przez transformację operacji,

- możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),
- możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)
- mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),
- mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),
- mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
- mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych,
- możliwość integracji z transakcjami bazy danych SBD, także rozproszonymi bez potrzeby pisania kodu.

48. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (hurtownia danych). System powinien umożliwiać pracę w dwóch trybach: wielowymiarowym (tworzenie kostek wielowymiarowych), tabelarycznym (wykorzystującym technologię in-memory BI). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.
49. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. System powinien pozwalać na integrację z relacyjną bazą danych –wymagana jest możliwość uruchomienia procesu wyliczenia agregacji zainicjowana poprzez dodanie rekordu do tabeli w relacyjnej bazy danych. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).
50. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
51. Narzędzia do zarządzania jakością danych - SBD powinien mieć wbudowane mechanizmy do zarządzania jakością danych w organizacji. W ramach tych funkcji powinien:
    - udostępniać funkcje do profilowania danych (analiza i raporty dotyczące jakości danych),
    - udostępniać funkcje do deduplikacji danych,
    - określać stopień poprawności wartości atrybutu i w przypadku błędnej wartości sugerować wartość poprawną do akceptacji przez użytkownika,
    - umożliwiać definiowanie osobnych reguł czyszczenia dla wybranych domen (typów atrybutów),
    - umożliwiać definiowanie złożonych domen (zestawu kilku atrybutów) oraz ocenę jakości danych na podstawie powiązań między tymi atrybutami (np. weryfikację poprawności danych adresowych złożonych z kodu pocztowego, miasta i ulicy),
    - pozwalać na ręczną korektę nieprawidłowych danych w dedykowanej aplikacji (bez konieczności programowania),

- umożliwiać eksport wyników badania (poprawnych i sugerowanych wartości) do pliku tekstowego lub bazy relacyjnej, eksport powinien obejmować wartości po korekcie oraz ewentualnie te przed korektą,
- przechowywać reguły walidujące i oceniające jakość danych w dedykowanej bazie danych (bazie wiedzy),
- umożliwiać uzupełnianie i rozszerzanie bazy wiedzy o dane referencyjne pochodzące z systemów zewnętrznych,
- zapewniać mechanizmy „uczenia się" bazy wiedzy, czyli w miarę realizacji kolejnych procesów ręcznego czyszczenia danych baza wiedzy powinna umożliwiać gromadzenie tych informacji na potrzeby kolejnych procesów,
- umożliwiać wykorzystanie bazy wiedzy w automatycznym procesie czyszczenia danych (powinien integrować się z narzędziami do ekstrakcji, transformacji i ładowania danych, dzięki czemu będzie można wykorzystać te mechanizmy w automatycznym procesie ładowania danych).

52. Możliwość zarządzania centralnymi słownikami danych - SBD powinien dostarczać narzędzia do przechowywania i zarządzania centralnym słownikiem danych (Master Data Management - MDM). System MDM powinien:
    - udostępniać narzędzia do wprowadzania, modyfikacji i wyszukiwania danych w słownikach,
    - umożliwiać wersjonowanie danych (śledzenie zmian wprowadzonych przez użytkowników z możliwością ich cofnięcia do wybranej wersji),
    - udostępniać mechanizm tworzenia i uruchamiania reguł walidujących poprawność danych w słownikach,
    - udostępniać narzędzia do administracji i kontroli uprawnień dostępu do danych w MDM,
    - udostępniać zestaw bibliotek (API programistyczne) z funkcjonalnościami MDM do wykorzystania w aplikacjach użytkownika,
    - umożliwiać eksport danych zgromadzonych w systemie MDM,
    - umożliwiać zarządzanie danymi podstawowymi z poziomu programu Microsoft Excel.
53. Wbudowany system analityczny powinien posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
54. Wbudowany system analityczny musi umożliwiać rejestrowanie zapytań wykonywanych przez użytkowników, a następnie umożliwiać na podstawie zgromadzonych informacji na automatyczną optymalizację wydajności systemu (np. automatyczne projektowanie agregacji pozwalające na przyspieszenie wykonywania najczęściej wykonywanych zapytań do bazy danych).
55. Wbudowany system analityczny powinien obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
56. Wbudowany system analityczny powinien udostępniać mechanizm zapisu danych przez użytkownika do kostek wielowymiarowych.
57. Wbudowany system analityczny powinien umożliwiać tworzenie perspektyw na bazie wielowymiarowej pozwalających ograniczyć widok dla użytkownika tylko do pewnego podzbioru obiektów dostępnych w całej bazie danych.
58. Wbudowany system analityczny powinien umożliwiać użytkownikom tworzenie analiz In-Memory, czyli przetwarzanie dużej liczby rekordów skompresowanych w pamięci RAM. Powinien umożliwiać tworzenie modeli wykorzystujących tabele pochodzące z wielu niezależnych źródeł danych i łączone między sobą relacjami.
59. Wbudowany system analityczny powinien udostępniać dedykowany język do tworzenia logiki biznesowej w modelu. Język ten powinien m.in. obsługiwać relacje utworzone między tabelami, mechanizmy time intelligence (operacje na datach i okresach) oraz zapewniać mechanizmy kontroli bezpieczeństwa i dostępu do danych na poziomie poszczególnych wierszy.

60. Wbudowany system analityczny powinien dostarczać kreatory modelowania złożonych procesów biznesowych, pozwalających w prosty sposób niezaawansowanym użytkownikom implementować złożone problemy analizy biznesowej w modelu analitycznym, czyniąc programowanie projektów BI przystępnym dla większej liczby osób i organizacji.

61. Wsparcie dla optymalizacji zapytań z modelu gwiazdy (fakty-wymiary) - SBD powinien udostępniać mechanizmy optymalizacji zapytań w modelu gwiazdy (tabela faktów łączona z tabelami wymiarów). Zapytania te często wykorzystywane są w hurtowniach danych i analizach wielowymiarowych. Ze względu na dużą liczbę danych wykorzystywanych w tego typu zapytaniach metody optymalizacji tego typu zapytań pozwalają znacząco zwiększyć wydajność przy tworzeniu rozwiązań hurtowni danych i wielowymiarowych struktur analitycznych (OLAP).

62. Wsparcie dla zapytań aktualizujących tabele faktów w modelach wielowymiarowych - SBD powinien udostępniać wbudowane mechanizmy pozwalające w łatwy i szybki sposób aktualizować zawartość tabel faktów (wykorzystywanych w modelach wielowymiarowych). Mechanizm ten powinien być dostępny z poziomu zapytań języka SQL obsługiwanego przez silnik bazy danych.

63. Aktywne buforowanie danych Proactive caching - SBD powinien udostępniać mechanizm odświeżania danych w strukturach wielowymiarowych, który wykrywa zmiany w systemach źródłowych i na bieżąco aktualizuje bazę wielowymiarową.

64. Wbudowany system analityczny powinien zapewniać mechanizmy dynamicznego security (każdy z użytkowników modelu powinien widzieć tylko swoje dane).

65. Wbudowany system analityczny powinien mieć wbudowaną funkcję importu tabelarycznych modeli danych wykorzystujących technologię in-memory BI i przygotowanych w aplikacji Microsoft Excel. Podczas procesu importu na serwerze model powinien być odtwarzany w postaci bazy danych.

66. Wbudowany system analityczny powinien umożliwiać zasilanie modelu tabelarycznego m.in. z następujących systemów źródłowych: bazy relacyjne, bazy wielowymiarowe, modele tabelaryczne, zbiory danych przechowywane w usługach chmury publicznej, pliki płaskie.

67. Wbudowany system analityczny powinien umożliwiać działanie modelu tabelarycznego w dwóch trybach – z użyciem buforowania (możliwe opóźnienie, ale większa wydajność) oraz bez użycia buforowania (zapytania użytkowników końcowych korzystających z modelu są przesyłane bezpośrednio do źródłowej bazy relacyjnej i zwracają najbardziej aktualną wersję danych).

68. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system powinien udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.

69. System analityczny powinien pozwalać na dodawanie własnych algorytmów oraz modułów wizualizacji modeli Data Mining.

70. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu. System powinien umożliwiać tworzenie takich wskaźników również w modelach danych wykorzystujących technologię in-memory BI.

71. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania powinien obsługiwać:

    - raporty parametryzowane,
    - cache raportów (generacja raportów bez dostępu do źródła danych),
    - cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),
    - współdzielenie predefiniowanych zapytań do źródeł danych,

- wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
- możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
- możliwość wizualizacji wskaźników KPI,
- możliwość wizualizacji danych w postaci obiektów sparkline.

72. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
73. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF, PowerPoint.
74. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.
75. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja) do dynamicznej listy odbiorców (pobieranej z bazy danych np. zapytaniem SQL).
76. Wbudowany system raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
77. Narzędzia do tworzenia raportów ad-hoc - SBD powinien udostępniać narzędzia do tworzenia raportów ad-hoc przez niezaawansowanych użytkowników. Tworzenie raportów powinno odbywać się w środowisku graficznym. Użytkownicy powinni mieć możliwość na publikowanie stworzonych raportów na serwerze w celu udostępnienia ich szerszemu gronu osób.
78. SBD musi posiadać wbudowane mechanizmy do obsług danych grafowych (struktur złożonych z węzłów i krawędzi - reprezentujących relacje między węzłami). System musi mieć wbudowane funkcje (dostępne z poziomu kodu SQL) do analizy powiązań między węzłami grafu oraz wyszukiwania najkrótszej ścieżki w grafie.
79. SBD musi posiadać mechanizmy klasyfikacji informacji przechowywanych w bazie danych w celu łatwej identyfikacji obszarów (obiektów) w bazie danych, gdzie składowane są dane wrażliwe. Mechanizm ten powinien umożliwiać przypisanie kolumnom w tabeli m.in. takich atrybutów jak: typ przechowywanych informacji oraz poziom wrażliwości danych. Dodatkowo SBD powinien udostępniać zestaw predefiniowanych raportów prezentujących m.in. listę sklasyfikowanych tabel i kolumn oraz liczbę tabel zawierających dane wrażliwe.
80. SBD musi mieć wbudowane mechanizmy umożliwiające wirtualizację danych (czyli przetwarzanie zapytań na danych niezależnie od miejsca przechowywania tych danych). W ramach wirtualizacji danych powinny być obsługiwane m.in. następujące platformy przechowywania danych źródłowych: MongoDB, Oracle, Teradata, Microsoft SQL Server, Hadoop, Azure Blob Storage.
81. SBD musi mieć wbudowane mechanizmy przetwarzania w sposób zrównoleglony skryptów analitycznych w językach R i Python.
82. SBD musi mieć możliwość tworzenia i trenowania modeli predykcyjnych w języku R w oparciu o dane z poszczególnych partycji w bazie danych.
83. SBD musi mieć możliwość budowy klastrów obliczeniowych dedykowanych do przetwarzania dużych zbiorów danych (big data, data lake) w oparciu o technologie SQL, Spark i HDFS. SBD musi umożliwiać odpytywanie danych z wielu źródeł, składowanie dużych zbiorów danych w HDFS, skalowanie wydajnościowe klastrów obliczeniowych wykorzystujące konteneryzację.

5.7 Win Remote Desktop Services CAL ALng SA UCAL

Licencje dostępowe do serwera Windows Server umożliwiające użytkownikom pracę w trybie terminalowym.

5.8 Win Server External Connector ALng SA

Licencje dostępowe do serwera Windows Server umożliwiające użytkownikom zewnętrznym dostęp do usług serwera.

5.9 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.

5.10 Win Server DC Core ALng SA 2L

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.

47. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
48. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
49. Możliwość budowania klastrów składających się z 64 węzłów.
50. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
51. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
52. Ochrona firmware przed atakami poprzez izolację hypervisora technologią Dynamic Root of Trust of Measurement (DRTM).
53. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
54. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    e. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    f. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    g. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    h. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
55. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
56. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
57. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
58. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
59. Możliwość wykorzystania standardu http/2.
60. Wbudowana obsługa TLS 1.3 włączona jako ustawienie standardowe..
61. Możliwość przechowywania wrażliwych danych i kluczy pod ochroną TPM 2.0.
62. Izolacja kernela od pozostałych komponentów systemu w oparciu zabezpieczenia bazujące na wirtualizacji (VBS) chroniąca przed metodami ataków wykorzystujących podatności używane przy „kopaniu” kryptowalut.
63. Dostępność usługi DNS-over-HTTPS (DoH) szyfrujących zapytania DNS przy użyciu HTTPS.
64. 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.
65. Szyfrowanie komunikacji i wspólnych zasobów wewnątrz klastra niezawodnościowego.
66. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
67. Wsparcie dla technologii Azure Arc pozwalające na traktowanie serwera zainstalowanego we własnym centrum przetwarzania jako zarządzalnego zasobu Azure.

68. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    c. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    d. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
69. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
70. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
71. Mechanizmy logowania w oparciu o:
    f. Login i hasło,
    g. Karty z certyfikatami (smartcard),
    h. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
    i. PIN zdefiniowany dla urządzenia,
    j. Rozpoznawanie twarzy.
72. 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.
73. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
74. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
75. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
76. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
77. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
78. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    ii. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    jj. 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.
    kk. Zdalna dystrybucja oprogramowania na stacje robocze.
    ll. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
    mm. 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.

nn. Szyfrowanie plików i folderów.

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

pp. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.

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

rr. Serwis udostępniania stron WWW.

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

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

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

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

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

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

yy. 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.

79. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.

80. Wsparcie dla rozwiązania dla rozwiązań kontenerowych dla aplikacji zgodnych z Kubernetes…

81. Możliwość wykorzystywania aplikacji kontenerowych wymagających wykorzystania Azure Active Directory bez dołączania hosta kontenerów do domeny.

82. Wsparcie migracji zasobów na dyskach do Azure.

83. 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.

84. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
85. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
86. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
87. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
88. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
89. Mechanizm konfiguracji połączenia VPN do platformy Azure.
90. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
91. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
92. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

5.11 Defender O365 P2 Sub Per User

Pakiet subskrypcji oprogramowania zaawansowanej ochrony pakietów Office 365 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.

5.12 Defender Endpoint P2 Sub Per User

Pakiet subskrypcji oprogramowania zaawansowanej ochrony urządzeń końcowych musi umożliwiać na 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. Udostępniać portal z aktualną informacją o wykrytych zagrożeniach, zarządzać ustawieniami ochrony wraz z kreowaniem raportów na te tematy i podejmować akcje eliminujące zagrożenia.
5. Wprowadzać dostęp zależny od roli użytkownika systemu ochrony.
6. Udostępniać wieloplatformowe API dla automatyzacji procesów związanych z ochroną zasobów.
7. Zbierać informację o zachowaniach systemu operacyjnego przechowując je w bezpiecznym odizolowanym zasobie i wskazując na nietypowe zachowania systemu.
8. Analizować dane na temat urządzenia i oprogramowania wykrywając zagrożenia i rekomendując działania zapobiegawcze.
9. Dzięki analizie danych wielu urządzeń i poznanych typach ataków identyfikować typ zagrożenia sygnalizując je w alertach.
10. W przypadku zagrożeń i ataków ustalać na bazie analizy ryzyka priorytety działań reaktywnych i proaktywnych w zakresie ochrony.
11. Redukować powierzchnię ataku poprzez wskazywanie właściwej konfiguracji urządzenia i systemu operacyjnego oraz ograniczanie dostępu do znanych jako niebezpieczne adresów IP, domen czy linków.
12. Tworzyć indeks „odporności urządzenia” poprzez tworzenie syntetycznych wskaźników odporności i wskazując konieczne zmiany w konfiguracji aby polepszyć te wskaźniki. Wskaźniki muszą obejmować między innymi:
    a. Aktualność poprawek bezpieczeństwa dla systemu operacyjnego
    b. Włączenie mechanizmów Exploit Guard
    c. Zdefiniowanie folderów dla działania Exploit Guard
    d. Skonfigurowanie raportów i akcji systemu antywirusowego
    e. Włączenie Credential Guard
    f. Właczenie ochrony BitLocker
    g. Szyfrowanie dysków
    h. Skonfigurowanie mechanizmów uwierzytelniania biometrycznego w tym Windows Hello
13. Wskazywać operatorom SOC najważniejsze zagrożenia i rekomendowane działania.

5.13 System Center DC Core ALng LSA 2L

Pakiet licencji oprogramowania zarządzania środowiskami serwerowymi uprawniać do zarządzania nielimitowaną liczbą środowisk systemu operacyjnego na tym serwerze fizycznym.

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.

5.14 Power BI Pro Sub Per User

Pakiet subskrypcji narzędzi prezentacji analizy danych musi być oparty na usługach obliczeniowych świadczonych z użyciem chmury publicznej spełniającej wymogi obowiązującego prawa. Opublikowane raporty i analizy powinny wykorzystywać moc obliczeniową chmury publicznej i w minimalnym stopniu obciążać komputery użytkowników końcowych.

1. System musi umożliwiać użytkownikom:

- import i łączenie danych z wielu różnych systemów źródłowych
- ładowanie danych do jednego spójnego modelu danych
- wzbogacanie modelu danych o dodatkowe pola obliczeniowe
- tworzenie raportów i wizualizacji danych w postaci tabel i wykresów przestawnych, interaktywnych raportów z możliwością dynamicznego i kontekstowego filtrowania danych,
- tworzenie animowanych wykresów pozwalających na śledzenie zmian i trendów w czasie,
- tworzenie wizualizacji z użyciem interaktywnych map geograficznych z nałożonymi warstwami analitycznymi (mapy powinni być wizualizowane w 2D oraz 3D z możliwością drążenia i powiększania w dowolnie wybranym punkcie mapy),
- tworzenie animowanych filmów prezentujących dane analityczne nałożone na na mapie geograficznej z możliwością dodawania do animacji komentarzy, opisów, wykresów oraz zdjęć,
- Wszystkie wyżej wymienione funkcje muszą być dostępne z poziomu jednej aplikacji raportowej z graficznym interfejsem użytkownika, bez konieczności dodatkowego programowania.

2. W celu zwiększenia wydajności przetwarzania system musi posiadać wbudowany mechanizm przetwarzania danych in-memory (w pamięci RAM komputera) oraz mechanizm kolumnowej kompresji danych. Wymienione mechanizmy in-memory muszą działać zarówno po stronie serwerowej (po opublikowaniu raportów na serwerze i udostępnieniu przez przeglądarkę WWW), jak również w

narzędziu raportowym na komputerze użytkownika (podczas przygotowywania modeli danych i raportów).

3. Narzędzie raportowe musi umożliwiać użytkownikowi pobieranie i łączenie danych z wielu źródeł w jednym modelu semantycznym. Proces pobierania danych w narzędziu raportowym musi umożliwiać użytkownikowi przekształcenie danych wejściowych i dostosowanie ich do postaci wymaganej w modelu semantycznym i raportach. Narzędzie raportowe musi mieć wbudowane gotowe funkcje i graficzne kreatory transformacji danych pozwalające na:

- usuwanie i kopiowanie kolumn wejściowych
- filtrowanie wierszy wejściowych na podstawie wartości z wybranych kolumn
- łączenie i rozdzielanie wartości w kolumnach (na podstawie wskazanego znaku separatora lub określonej liczby znaków)
- konwersję typów danych (tekstowy, liczbowy, daty)
- automatyczną zamianę wielkości liter w danych wejściowych
- automatyczne usuwanie duplikatów wartości we wskazanej kolumnie
- automatyczne zastępowanie wartości w kolumnach inną wskazaną przez użytkownika
- automatyczną konwersję danych z formatu JSON
- automatyczne wyliczanie agregacji (grupowanie danych według danej kolumny)
- automatyczne wykonywanie operacji przekształcenia wierszy w kolumny i kolumn w wiersze (pivot/unpivot)
- automatyczne łączenie wielu tabel o takiej samej strukturze kolumn w jedną tabelę (UNION)
- automatyczne złączenie dwóch różnych tabel w jedną na podstawie wskazanych wspólnych kolumn dla obu tabel (kluczy złączenia)

4. Zastosowane przez użytkownika transformacje danych (zapytanie) muszą być pamiętane w narzędziu, jako sekwencja kolejno następujących po sobie czynności (etapów). Użytkownik musi mieć możliwość przejścia do dowolnego z kroków procesu transformacji danych i obejrzenia danych sprzed zastosowania danego kroku.

5. Zdefiniowane kroki transformacji danych powinny być zapamiętywane w postaci automatycznie generowanego skryptu, który zaawansowani użytkownicy mogą modyfikować i powielać.

6. System musi udostępniać funkcję katalogu zapytań, w którym autorzy zapytań (transformacji danych) udostępniają efekty swojej pracy dla innych użytkowników. Użytkownicy katalogu zapytań, z poziomu narzędzia raportowego, muszą mieć możliwość wyszukania i wykorzystania interesującego ich zapytania na potrzeby zasilania danymi własnych analiz i raportów. W katalogu zapytań musi istnieć:

- możliwość nadawania uprawnień dostępu do zapytania dla poszczególnych użytkowników lub grup użytkowników
- możliwość podglądu w wyszukiwarce zapytań wyniku zwracanego przez określone zapytanie (zanim jeszcze wynik zapytania zostanie załadowany do narzędzia raportowego i modelu danych).
- możliwość wprowadzenia nazwy i opisu biznesowego określonego zapytania w celu łatwiejszego wyszukiwania
- możliwość dołączenia adresu URL do dokumentacji opisującej zawartość merytoryczną zapytania i wyników, które ono zwraca
- dostęp do statystyk i monitoringu częstości wyszukiwania i wykorzystania przez użytkowników opublikowanych zapytań.

7. Narzędzie raportowe musi mieć wbudowane sterowniki do pobierania danych, co najmniej z następujących źródeł: pliki tekstowe, pliki CSV, pliki XML, pliki Excel, strony internetowe (podając adres URL takiej strony), bazy relacyjne (Microsoft SQL Server, Oracle, IBM DB2, MySQL, PostgreSQL, Sybase, Teradata), listy Sharepoint, Facebook, Active Directory, SAP Business Objects, Microsoft Azure, OData Feed, klastry Hadoop, ODBC. Dodatkowo system musi umożliwiać bezpośrednio w

narzędziu raportowym wyszukiwanie i importowanie zbiorów danych dostępnych w internecie (wyszukiwanie na podstawie słów kluczowych i zwrotów podawanych przez użytkownika).

8. System musi umożliwiać dostęp do danych oraz wykonywanie analiz z wykorzystaniem zapytań w języku naturalnym. Użytkownik musi mieć możliwość wpisywania pytania w języku naturalnym bezpośrednio na portalu, a jako odpowiedź system powinien zwracać wyniki w formie tabel, wykresów lub map geograficznych. Sposób wizualizacji danych powinien być automatycznie dobierany przez system w celu optymalnej i czytelnej prezentacji wyników (np. w przypadku zapytań o dane związane z położeniem geograficznym system powinien automatycznie prezentować wyniki nałożone na mapie geograficznej). Jednocześnie użytkownik musi mieć możliwość dalszej zmiany sposobu wizualizacji otrzymanych wyników tak, aby dostosować je do własnych preferencji (np. zamiana danych prezentowanych w formie mapy geograficznej na tabelę, wykres kołowy, liniowy itp.). Użytkownik musi mieć możliwość wyboru modelu danych, w kontekście którego uruchamiane są zapytania w języku naturalnym.

9. System musi zapewniać użytkownikom możliwość umieszczenia/przypięcia na portalu często wykorzystywanych zapytań zdefiniowanych w języku naturalnym. Musi istnieć możliwość umieszczania tych zapytań w postaci graficznego interfejsu obiektowego, tzn. pod każdym obiektem graficznym powinno być podpięte pytanie, które po kliknięciu na dany obiekt jest automatycznie uruchamiane, a jego wyniki prezentowane są w oknie przeglądarki w formie interaktywnego raportu. Użytkownik (bezpośrednio w przeglądarce) musi mieć możliwość wprowadzenia zmiany koloru obiektów graficznych, dodania na obiektach własnej grafiki (np. poprzez wstawienie źródłowego adresu URL do grafiki dostępnej w sieci) oraz zmiany rozmiaru obiektów.

10. System musi umożliwiać publikację modeli danych oraz raportów bezpośrednio na portalu. Po udostępnieniu raportu na portalu dla użytkowników powinny być dostępne takie informacje, jak: tytuł raportu, data i czas opublikowania raportu, nazwa użytkownika publikującego raport oraz graficzny podgląd zawartości raportu.

11. Użytkownicy muszą mieć możliwość wyboru i oznaczenia wybranych raportów, jako swoich ulubionych. Ulubione raporty użytkownika są automatycznie oznaczane gwiazdką, a jednocześnie prezentowane w osobnej części portalu, dedykowanej do prezentacji jedynie ulubionych raportów bieżącego użytkownika.

12. System musi udostępniać dedykowany język do tworzenia logiki biznesowej w modelu semantycznym. Język ten musi m.in. obsługiwać relacje utworzone między tabelami, mechanizmy operacji na datach i okresach (time intelligence), agregacje danych, wyrażenia warunkowe, hierarchie, filtrowanie danych, funkcje matematyczne i statystyczne. Narzędzia muszą mieć wbudowany mechanizm podpowiadania składni wyrażeń i funkcji w tym języku.

13. System musi umożliwiać automatyczną synchronizację i odświeżanie opublikowanych raportów, zarówno zasilanych ze źródeł internetowych (w tym z chmury publicznej), jak również ze źródeł i baz danych przechowywanych we własnym centrum przetwarzania danych.

14. System musi udostępniać aplikację dedykowaną dla urządzeń mobilnych przystosowaną do prezentacji raportów z użyciem interfejsu dotykowego.

15. Raporty oznaczone jako ulubione na portalu raportowym powinny być również prezentowane w sekcji raportów ulubionych w aplikacji.

5.15 Win Server Standard Core ALng SA 2L

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.

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

48. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.

49. Możliwość budowania klastrów składających się z 64 węzłów.

50. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
51. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
52. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
53. 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).
54. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
55. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
56. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
57. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
58. Możliwość wykorzystania standardu http/2.
59. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
60. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
61. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
62. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
63. 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),
64. 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.
65. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
66. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
67. Ochrona firmware przed atakami poprzez izolację hypervisora technologią Dynamic Root of Trust of Measurement (DRTM).
68. Możliwość przechowywania wrażliwych danych i kluczy pod ochroną TPM 2.0
69. Izolacja kernela od pozostałych komponentów systemu w oparciu zabezpieczenia bazujące na wirtualizacji (VBS) chroniąca przed metodami ataków wykorzystujących podatności używane przy „kopaniu” kryptowalut.

70. Wbudowana obsługa TLS 1.3 włączona jako ustawienie standardowe..
71. Dostępność usługi DNS-over-HTTPS (DoH) szyfrujących zapytania DNS przy użyciu HTTPS.
72. 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.
73. Szyfrowanie komunikacji i wspólnych zasobów wewnątrz klastra niezawodnościowego.
74. Wsparcie dla technologii Azure Arc pozwalające na traktowanie serwera zainstalowanego we własnym centrum przetwarzania jako zarządzalnego zasobu Azure.
75. Możliwość wykorzystywania aplikacji kontenerowych wymagających wykorzystania Azure Active Directory bez dołączania hosta kontenerów do domeny.
76. Wsparcie migracji zasobów na dyskach do Azure.
77. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
78. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
79. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
80. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

    zz. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

    aaa. 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.

    bbb. Zdalna dystrybucja oprogramowania na stacje robocze.

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

    ddd. 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.

    eee. Szyfrowanie plików i folderów.

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

    ggg. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.

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

iii. Serwis udostępniania stron WWW.

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

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

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

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

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

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

ppp. 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.

81. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
82. Wsparcie dla rozwiązania Kubernetes.
83. 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.
84. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
85. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
86. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
87. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
88. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
89. Mechanizm konfiguracji połączenia VPN do platformy Azure.
90. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
91. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
92. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

5.16 Project P3 Sub 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.