Gdańskie Centrum Informatyczne

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA
(SIWZ)

w postępowaniu o udzielenie zamówienia publicznego prowadzonym
w trybie przetargu nieograniczonego
pn.

Dostawa Produktów Microsoft lub Produktów równoważnych w ramach środowiska pracy grupowej.

(Numer postępowania ZP/6/D/2019/K)

o wartości przekraczającej kwotę określoną w przepisach wydanych na podstawie art. 11 ust. 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych

ZATWIERDZAM

Maria Bollin
Dyrektor
Gdańskiego Centrum Informatycznego

Gdańsk, marzec 2019 r.

Spis treści:

I. Zamawiający.
II. Tryb udzielenia zamówienia.
III. Informacje ogólne.
IV. Przedmiot zamówienia.
V. Termin i miejsce wykonania zamówienia.
VI. Warunki udziału w postępowaniu oraz podstawy wykluczenia.
VII. Wykaz oświadczeń lub dokumentów, potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.
VIII. Informacje o oświadczeniach i dokumentach.
IX. Opis sposobu przygotowywania ofert. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.
X. Wymagania dotyczące wadium.
XI. Termin związania ofertą.
XII. Termin składania i otwarcia ofert.
XIII. Opis sposobu obliczenia ceny.
XIV. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty.
XV. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.
XVI. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.
XVII. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy, jeżeli Zamawiający wymaga od Wykonawcy, aby zawarł z nim umowę w sprawie zamówienia publicznego na takich warunkach.
XVIII. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia.
XIX. Załączniki.

ROZDZIAŁ I. ZAMAWIAJĄCY

1. **Oznaczenie Zamawiającego:**

   Gdańskie Centrum Informatyczne (jednostka organizacyjna działająca w imieniu Gminy Miasta Gdańska, ul. Nowe Ogrody 8/12, 80-803 Gdańsk NIP: PL 583 00 11 969)
   ul. Prof. Witolda Andruszkiewicza 5
   80-601 Gdańsk
   REGON: 367708720
   www.gci.gdansk.pl
   Adres strony internetowej, na której dostępna jest Specyfikacja Istotnych Warunków Zamówienia: www.gci.gdansk.pl (zakładka Biuletynu Informacji Publicznej).
   Godziny urzędowania: poniedziałek, wtorek, czwartek: w godzinach 8:00 – 16:00, środa w godzinach: 8:00 – 17:00, piątek: w godzinach 8:00 – 15:00.

ROZDZIAŁ II. TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie o udzielenie zamówienia publicznego, prowadzone jest na podstawie przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 poz. 1986) zwanej dalej „ustawą Pzp", wydanych na podstawie tej ustawy rozporządzeń wykonawczych oraz zgodnie z wymaganiami określonymi w niniejszej Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej „SIWZ".
2. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie przetargu nieograniczonego art. 39 i nast. ustawy Pzp.
3. Wartość zamówienia przekracza kwotę określoną w przepisach wydanych na podstawie art. 11 ust. 8 ustawy Pzp.

ROZDZIAŁ III. INFORMACJE OGÓLNE

1. Zamawiający ze względu na specyfikę przedmiotu zamówienia **nie dopuszcza możliwości** składania ofert częściowych.
2. Zamawiający **nie dopuszcza** składania ofert wariantowych.
3. Zamawiający **nie przewiduje** aukcji elektronicznej.
4. Zamawiający **nie przewiduje** udzielenia zamówień uzupełniających, o których mowa w art. 67 ust. 1 pkt 6 ustawy Pzp.
5. **Przygotowując ofertę, Wykonawca winien dokładnie zapoznać się z zawartością wszystkich dokumentów składających się na niniejszą specyfikację, którą należy odczytywać wraz z ewentualnymi modyfikacjami i zmianami wnoszonymi przez Zamawiającego.**
6. **Zamawiający może najpierw dokonać oceny ofert, a następnie zbadać, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu (na podstawie art. 24aa ust. 1 ustawy Pzp).**
7. Oferta złożona w niniejszym postępowaniu musi być jednoznaczna i kompleksowa, tj. obejmować cały asortyment przedmiotu zamówienia. Oferowany przedmiot zamówienia musi spełniać wymogi Zamawiającego. **Przedmiot zamówienia musi być kompletny, po uruchomieniu musi gotowy do pracy zgodnie z przeznaczeniem, bez dodatkowych zakupów po stronie Zamawiającego.** Wykonawca na etapie realizacji zamówienia, wykonuje przedmiot zamówienia zgodnie z wymogami Zamawiającego. Wykonawca realizuje przedmiot zamówienia własnymi środkami.
8. Wykonawca zobowiązany jest do złożenia oferty, której treść pozwoli Zamawiającemu na zweryfikowanie jej pod względem zgodności z treścią SIWZ. Treść oferty Wykonawcy musi odpowiadać treści Specyfikacji Istotnych Warunków Zamówienia.
9. Wszelkie koszty związane z wykonaniem przedmiotu zamówienia ponosi Wykonawca.
10. Szczegółowe wymagania i informacje dotyczące realizacji przedmiotu zamówienia oraz warunków płatności zawiera Załącznik nr 9 do SIWZ – **Istotne postanowienia umowy.**
11. **Podwykonawcy:**
    1) Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy, zgodnie z art. 36a ust. 1 ustawy Pzp.
    2) Zamawiający informuje, iż nie dokonuje zastrzeżenia obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia – w myśl art. 36a ust. 2 ustawy Pzp.

3) Zamawiający żąda wskazania przez Wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, i podania przez Wykonawcę firm podwykonawców. Powyższe powinno zostać dokonane poprzez oświadczenie Wykonawcy, złożone w wyznaczonym miejscu w druku formularza oferty.
4) Zamawiający żąda, aby przed przystąpieniem do wykonania zamówienia Wykonawca, o ile są już znane, podał nazwy albo imiona i nazwiska oraz dane kontaktowe podwykonawców i osób do kontaktu z nimi, zaangażowanych w realizację przedmiotowej usługi. Wykonawca zawiadamia Zamawiającego o wszelkich zmianach danych, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazuje informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację usług.
5) W przypadku powierzenia realizacji umowy podwykonawcy, Wykonawca ponosi pełną odpowiedzialność wobec Zamawiającego za jego działania lub zaniechania.
6) Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 22 a ust. 1 ustawy Pzp, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, iż proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.

12. **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – dalej: „RODO”.**
   1) Wykonawca biorący udział w postępowaniu winien znać i przestrzegać wszelkich obowiązków wynikających z obowiązujących przepisów o ochronie danych osobowych, w tym przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
   2) Wykonawca winien wypełniać obowiązki informacyjne przewidziane w artykule 13 lub artykule 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu;
   3) Zamawiający zastrzega, że przekazywane przez Wykonawcę dane osobowe mogą być wykorzystane wyłącznie w celach związanych z niniejszym postępowaniem;
   4) Wykonawca biorący udział w postępowaniu w treści formularza oferty składa stosowne oświadczenie w zakresie przepisów RODO;
   5) Niniejsze postanowienia dotyczące RODO mają zastosowanie również wobec podwykonawcy. Zamawiający zastrzega prawo zażądania stosowanego oświadczenia od podwykonawcy w zakresie, o którym mowa w niniejszym ustępie.
   6) **Zmawiający, zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej RODO, informuje że:**
      a. administratorem Pani/Pana danych osobowych jest Gdańskie Centrum Informatyczne (dalej GCI) z siedzibą w Gdańsku (80-601) przy ul. Prof. Witolda Andruszkiewicza 5.
      b. w GCI powołany został inspektor ochrony danych (IOD), z którym można kontaktować się:
         - listownie na adres: Gdańskie Centrum Informatyczne ul. Prof. Witolda Andruszkiewicza 5, 80-601 Gdańsk;
         - drogą elektroniczną na adres e-mail: iod/gci@gdansk.gda.pl;
      c. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego,
      d. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp”;
      e. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
      f. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym

z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

g. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
h. posiada Pani/Pan:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych, z zastrzeżeniem, że skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników;
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO, z zastrzeżeniem, że prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego;
   - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
i. nie przysługuje Pani/Panu:
   - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

ROZDZIAŁ IV. PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zamówienia jest dostawa Produktów Microsoft lub Produktów równoważnych następującego rodzaju:
   1) Licencje,
   2) Licencje subskrypcyjne,
   3) Usługi.
2. Szczegółowy zakres zamówienia określa Opis przedmiotu zamówienia (OPZ) - Załącznik nr 8 do SIWZ.
3. Warunki realizacji przedmiotu zamówienia zostały określone w niniejszej SIWZ oraz w Istotnych Postanowieniach Umowy (IPU) – Załącznik nr 9 do SIWZ.
4. Podmiotem na rzecz którego dostarczane są Produkty wskazane w ust. 1 jest Gmina Miasta Gdańska.
5. Przedmiot zamówienia w niniejszym postępowaniu został podzielony na zamówienie podstawowe oraz zamówienia objęte prawem opcji.
6. Warunki i zasady korzystania z prawa opcji:
   1) Prawem opcji objęte są Produkty wskazane w Opisie przedmiotu zamówienia w prognozowanej liczbie, przy czym Zamawiający będzie uprawniony do swobodnej zmiany liczby Produktów danego rodzaju w ramach zamówienia objętego prawem opcji (w ramach listy produktów) pod warunkiem, że zmiany te nie wpłyną na łączną wartość zamówienia objętego prawem opcji, które wynikać będzie z oferty Wykonawcy.
   2) Zamawiający może udzielić zamówień w ramach prawa opcji w przypadku pojawienia się zapotrzebowania.
   3) Zamawiający ma prawo do skorzystania z prawa opcji w zakresie pełnym, częściowym lub nie skorzystać z tego prawa. Zamawiający zastrzega sobie prawo zrealizowania zamówienia tylko w zakresie zamówienia podstawowego i Wykonawca nie będzie wysuwał w stosunku do Zamawiającego żadnych roszczeń z tego tytułu.
   4) Każdorazowo zamówienie objęte prawem opcji będzie realizowane przez Wykonawcę na podstawie Oświadczenia Zamawiającego. Procedura dotycząca prawa opcji oraz sposób rozliczeń określono w IPU.

7. Kody klasyfikacji Wspólnego Słownika Zamówień (CPV):
   1) 48517000-5 – Pakiety oprogramowania Informatycznego;
   2) 48310000-4 – Pakiety oprogramowania do tworzenia dokumentów.

8. Równoważność:
   1) Zamawiający dopuszcza możliwość złożenia oferty Produktów równoważnych w zakresie zamówienia podstawowego i zamówienia objętego prawem opcji, zgodnie z Opisem przedmiotu zamówienia stanowiącym Załącznik nr 8 do SIWZ. Za Produkt równoważny Zamawiający uzna produkt o cechach (parametrach) zgodnych z Produktem Microsoft lub lepszych niż Produkt określony w Opisie przedmiotu zamówienia.
   2) Wykonawca w formularzu cenowym winien wskazać jaki rodzaj Produktów oferuje, tj. Produkty Microsoft bądź Produkty równoważne. W przypadku, gdy Wykonawca oferuje Produkty równoważne Zamawiający wymaga, aby wraz z ofertą Wykonawca dołączył dokumenty potwierdzające, że oferowane przez niego produkty spełniają wymagania w zakresie równoważności, zgodnie z Opisem przedmiotu zamówienia.
   3) Zgodnie z dyspozycją art. 30 ust. 5 ustawy Pzp na Wykonawcy ciąży obowiązek, wykazania, że Produkty równoważne spełniają wymagania postawione przez Zamawiającego.
   4) Zamawiający zastrzega sobie w przypadku jakichkolwiek wątpliwości, prawo sprawdzenia pełnej zgodności warunków i zakresu równoważności oferowanych Produktów równoważnych. W takim wypadku, Zamawiający wezwie Wykonawców do przedstawienia dodatkowych dokumentów danego Produktu w celu potwierdzenia spełnienia wymagań w zakresie równoważności oraz próbek oferowanych Produktów, dla celów wykonania testów w środowiskach Zamawiającego. Sprawdzenie to, będzie polegać na przeprowadzeniu testów w warunkach odzwierciedlających środowiska produkcyjne na sprzęcie Zamawiającego, z użyciem urządzeń peryferyjnych Zamawiającego, na plikach, arkuszach, bazach danych i dokumentach Zamawiającego. Testowane będą opisane w wymaganiach SIWZ funkcje Produktów, wobec których to funkcji Zamawiający powziął wątpliwość o ich zgodności z wymaganiami SIWZ. W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby Zamawiającego w terminie 3 roboczych dni od daty otrzymania wezwania, po jednym egzemplarzu wskazanego Produktu wobec którego Zamawiający powziął wątpliwość co do jego zgodności z wymaganiami SIWZ. W odniesieniu do tych Produktów mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Jednocześnie Zamawiający zastrzega sobie możliwość odwołania się do oficjalnych, publicznie dostępnych stron internetowych Producenta weryfikowanego przedmiotu oferty. Nieprzedłożenie oferowanych Produktów równoważnych do przetestowania w ww. terminie zostanie potraktowane, jako negatywny wynik sprawdzenia. Po wykonaniu testów, dostarczone do testów egzemplarze Produktów będą zwrócone Wykonawcy na jego pisemny wniosek.
   5) Negatywny wynik sprawdzenia oferty w zakresie równoważności oferowanych Produktów skutkować będzie odrzuceniem tej oferty.

ROZDZIAŁ V. TERMIN I MIEJSCE WYKONANIA ZAMÓWIENIA

1. **Termin realizacji zamówienia.**
   Maksymalny termin realizacji zamówienia to 36 miesięcy. Zamawiający w treści Opisu przedmiotu zamówienia określił termin realizacji przedmiotu zamówienia dla danego Produktu.
2. **Miejsce realizacji przedmiotu zamówienia.**
   Wykonawca dostarczy wszelkie dane do rozpoczęcia realizacji przedmiotu zamówienia w sposób określony w Opisie przedmiotu zamówienia i w treści Istotnych postanowień umowy.

ROZDZIAŁ VI. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ PODSTAWY WYKLUCZENIA

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu oraz spełniają warunki udziału w postępowaniu (o ile zostały przez Zamawiającego określone).
2. **Podstawy wykluczenia:**
   1) Z postępowania o udzielenie zamówienia Zamawiający wykluczy Wykonawcę, w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych w **art. 24 ust. 1 ustawy Pzp.**

2) Podstawy wykluczenia, o których mowa w art. 24 ust. 5 ustawy Pzp: Zamawiający przewiduje wykluczenie Wykonawcy na podstawie **art. 24 ust. 5 pkt. 1 ustawy Pzp.**

3. **Warunki udziału w postępowaniu:**
   1) W zakresie kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów: Zamawiający nie określa szczegółowego warunku w tym zakresie.
   2) W zakresie sytuacji ekonomicznej lub finansowej: Zamawiający nie określa szczegółowego warunku w tym zakresie.
   3) **W zakresie zdolności technicznej lub zawodowej.**
      Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie zrealizował minimum jedną dostawę licencji subskrypcyjnych należących do środowiska pracy grupowej dla minimum 500 użytkowników, wśród których znajdowały się pakiety do pracy biurowej.
      W przypadku usług okresowych lub ciągłych Zamawiający uzna powyższy warunek za spełniony jeżeli Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie już wykonał w sposób należyty w ramach większego zamówienia dostawę licencji subskrypcyjnych należących do środowiska pracy grupowej dla minimum 500 użytkowników wśród których znajdowały się pakiety do pracy biurowej.
4. Zgodnie z art. 24 ust. 12 ustawy Pzp, Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia.
5. Ocena spełnienia warunków udziału w postępowaniu i niepodleganie wykluczeniu zostaną dokonane na podstawie oświadczeń i dokumentów wskazanych w niniejszej SIWZ.

ROZDZIAŁ VII. WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW WYKLUCZENIA

1. POTWIERDZENIE BRAKU PODSTAW DO WYKLUCZENIA Z UDZIAŁU W POSTĘPOWANIU ZAMAWIAJĄCY ŻĄDA ZASTĘPUJĄCYCH DOKUMENTÓW.

W celu potwierdzenia przez Wykonawcę braku podstaw do wykluczenia Zamawiający żąda następujących dokumentów:

1) SKŁADANYCH WRAZ Z OFERTĄ W TERMINIE WSKAZANYM W ROZDZIALE XII UST. 1 (w terminie składania ofert):
   a. **Jednolitego Europejskiego Dokumentu Zamówienia (dalej JEDZ):**
      - Do oferty Wykonawca dołącza aktualne na dzień złożenia oświadczenie w zakresie wskazanym przez Zamawiającego w niniejszej SIWZ lub Ogłoszeniu o zamówieniu. Informacje zawarte w oświadczeniu stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. Wykonawca składa niniejsze oświadczenie w formie JEDZ, zgodnie z przyjętym wzorem (Rozporządzenie wykonawcze Komisji Europejskiej wydane na podstawie Dyrektywy Komisji Europejskiej 2014/24/UE – art. 59 ust. 2 i Dyrektywy 2014/25/UE – art. 80 ust. 3).
      - Zamawiający zaleca zapoznanie się z instrukcją udostępnioną przez Urząd Zamówień Publicznych: https://www.uzp.gov.pl/baza-wiedzy/jednolity-europejski-dokument-zamowienia https://www.uzp.gov.pl/__data/assets/pdf_file/0015/32415/Jednolity-Europejski-Dokument-Zamowienia-instrukcja.pdf
      - Wykonawca może ograniczyć się do uzupełnienia sekcji α – ogólne oświadczenie dotyczące wszystkich kryteriów kwalifikacji, w części IV (kryteria kwalifikacji). Wykonawca nie jest zobowiązany do wypełniania żadnej z pozostałych sekcji w części IV. JEDZ.

2) SKŁADANYCH W TERMINIE WSKAZANYM W ART. 24 UST. 11

Wykonawca **w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy Pzp (informacji z otwarcia ofert),** przekaże Zamawiającemu:

a. **Oświadczenie o przynależności albo braku przynależności do tej samej grupy kapitałowej;** w przypadku przynależności do tej samej grupy kapitałowej Wykonawca może złożyć wraz z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w przedmiotowym postępowaniu.

3) SKŁADANYCH NA PODSTAWIE WEZWANIA ZAMAWIAJĄCEGO:
Zamawiający wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 10 dni, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy Pzp, tj:

a. **Informacji z Krajowego Rejestru Karnego** w zakresie określonym w art. 24 ust. 1 pkt. 13, 14, 21 ustawy Pzp wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
b. **Oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne** albo – w przypadku wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności.
c. **Oświadczenia Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne.**
d. **Oświadczenia Wykonawcy o niezaleganiu z opłacaniem podatków i opłat lokalnych,** o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2016 r. poz. 716).
e. **Odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji,** w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy Pzp.

2. WYKAZANIE SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU.

W celu potwierdzenia spełniania przez Wykonawcę warunków udziału w postępowaniu w zakresie zdolności technicznej lub zawodowej Zamawiający żąda następujących dokumentów:

1) **Wykazu dostaw** wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane,
2) **Dowodów określających czy te dostawy zostały wykonane lub są wykonywane należycie**, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.
3) **Dokumenty wskazane powyżej w pkt. 1 oraz 2 Wykonawca będzie zobowiązany przedłożyć na wezwanie Zamawiającego, w terminie o którym mowa w ust. 1 pkt. 3 niniejszego rozdziału.**

ROZDZIAŁ VIII. INFORMACJE O OŚWIADCZENIACH I DOKUMENTACH.

1. WYKONAWCY WSPÓLNIE UBIEGAJĄCY SIĘ O UDZIELENIE ZAMÓWIENIA:

1) W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia do oferty należy dołączyć dokument ustanawiający pełnomocnika do reprezentowania ich w

postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie niniejszego zamówienia publicznego zgodnie z art. 23 ust. 2 ustawy Pzp.

2) W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców odrębne oświadczenia i dokumenty, o których mowa w rozdziale VII. ust. 1.

2. WYKONAWCY, KTÓRZY MAJĄ SIEDZIBĘ POZA TERYTORIUM RZECZYPOSPOLITEJ POLSKIEJ:

1) **Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej zamiast dokumentów o których mowa w ust. 1 pkt 3) rozdziału VII:**
   a. Pkt 3) lit. a, składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy Pzp;
   b. Pkt 3) lit. e, składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji ani nie ogłoszono upadłości.
2) Dokumenty, o których mowa w ust. 2 pkt 1) lit. a i b, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
3) Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w ust. 2 pkt 1) lit. a, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce za-mieszkania Wykonawcy lub miejsce zamieszkania tej osoby. Przepis pkt. 2) stosuje się.
4) W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę, Zamawiający może zwrócić się do właściwych organów odpowiednio kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.
5) Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w rozdziale VII ust. 1 pkt 3) lit. a, składa dokument, o którym mowa w ust. 2 pkt 1) lit. a niniejszego rozdziału, w zakresie określonym w art. 24 ust. 1 pkt 14 i 21 ustawy Pzp. Jeżeli w kraju, w którym miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby. Przepis pkt 2) stosuje się.
6) W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę, zamawiający może zwrócić się do właściwych organów kraju, w którym miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.

3. INNE PODMIOTY NA ZASOBY KTÓRYCH MOŻE POWOŁAĆ SIĘ WYKONAWCA:

1) Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu – o ile zostały określone w treści SIWZ (w rozdziale VI), w stosownych sytuacjach oraz w odniesieniu do zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
2) W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują usługi, do realizacji których te zdolności są wymagane.
3) W sytuacji gdy Wykonawca polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując przedmiotowe zamówienie będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.
4) Wykonawca, który polega na sytuacji finansowej lub ekonomicznej innych podmiotów, odpowiada solidarnie z podmiotem, który zobowiązał się do udostępnienia zasobów, za szkodę

poniesioną przez Zamawiającego powstałą w skutek nieudostępnienia tychże zasobów, chyba że za nieudostępnienie zasobów nie ponosi winy.

5) W przypadku gdy Wykonawca polega na zasobach innych podmiotów do oferty zobowiązany jest dołączyć oświadczenie o którym mowa w rozdz. VII. ust. 1 pkt 2 niniejszej SIWZ dotyczące każdego z podmiotów.
6) Dokument z którego będzie wynikało zobowiązanie innego podmiotu do oddania do dyspozycji Wykonawcy niezbędnych na potrzeby wykonania niniejszego zamówienia zasobów. Dokument ten wymagany jest od każdego podmiotu na zasoby którego powołuje się Wykonawca.
7) Dokument zobowiązania do oddania do dyspozycji zasobów winien zawierać następujące informacje:
   a. nazwę podmiotu, który udostępnia swoje zasoby,
   b. nazwę Wykonawcy na rzecz którego inny podmiot udostępnia swoje zasoby,
   c. zakres udostępnianych Wykonawcy zasobów przez podmiot,
   d. w jaki sposób Wykonawca wykorzysta zasoby innego podmiotu przy realizacji niniejszego zamówienia,
   e. zakres udziału innego podmiotu przy realizacji niniejszego zamówienia publicznego,
   f. okres w którym inny podmiot będzie uczestniczył w realizacji niniejszego zamówienia,
   g. dokument zobowiązania winien być złożony w oryginale, w postaci dokumentu elektronicznego.
8) Zamawiający podda ocenie, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13–22 i art. 24 ust. 5 pkt 1 ustawy Pzp, o których mowa w niniejszej SIWZ.
9) W przypadku gdy zdolności techniczne lub zawodowe podmiotu, na którego zdolnościach polega Wykonawca biorący udział w postępowaniu, nie potwierdzają spełnienia przez Wykonawcę warunków udziału w postępowaniu lub w sytuacji w której zachodzą wobec tych podmiotów podstawy do wykluczenia, Zamawiający będzie żądał, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami bądź zobowiązał się do osobistego wykonania odpowiedniej części zamówienia, jeżeli wykaże zdolności techniczne lub zawodowe lub sytuację finansową lub ekonomiczną.

4. INFORMACJE DODATKOWE:

1) Zgodnie z art. 26 ust. 6 ustawy Pzp, Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3, tj. spełnianie warunków udziału w postępowaniu i brak podstaw wykluczenia z postępowania, jeżeli Zamawiający posiada oświadczenia lub dokumenty dotyczące tego Wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570).
2) W przypadku wskazania przez Wykonawcę dostępności oświadczeń lub dokumentów wymaganych w niniejszym postępowaniu, o których mowa w § 2, § 5 i § 7 Rozporządzenia Ministra Rozwoju z dnia 27.07.2016 r. w sprawie dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia (dalej „Rozporządzenia"), w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych zamawiający pobiera samodzielnie z tych baz danych wskazane przez wykonawcę oświadczenia lub dokumenty.
3) W przypadku wskazania przez Wykonawcę oświadczeń lub dokumentów wymaganych w niniejszym postępowaniu , o których mowa w § 2, § 5 i § 7 Rozporządzenia, które znajdują się w posiadaniu zamawiającego, w szczególności oświadczeń lub dokumentów przechowywanych przez Zamawiającego zgodnie z art. 97 ust. 1 ustawy, zamawiający w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 ustawy, korzysta z posiadanych oświadczeń lub dokumentów, o ile są one aktualne.
4) W związku z treścią pkt 1-3 niniejszego ustępu, Wykonawca zobowiązany jest w wyznaczonym miejscu w formularzu oferty do wskazania z jakiego dokumentu może skorzystać Zamawiający w niniejszym postępowaniu (nazwa innego adres strony internetowej pod którym dostępny jest właściwy dokument, informacja o postępowaniu w ramach którego Wykonawca złożył wymagany dokument).
5) W przypadku, gdy prawo osoby (osób) do reprezentacji Wykonawcy nie wynika z dokumentu (dokumentów), które Zamawiający może uzyskać w za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z

dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352), Wykonawca winien wraz z ofertą złożyć pełnomocnictwo do reprezentacji Wykonawcy.

6) **Jeżeli wadium w niniejszym postępowaniu zostało wniesione w innej formie niż w pieniądzu, wówczas do ofert dołączyć należy oryginał gwarancji bankowej lub poręczenia.**
7) Zamawiający wezwie Wykonawców, którzy w ofercie nie złożą oświadczeń lub dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, lub którzy nie złożą wymaganych pełnomocnictw albo złożą wadliwe pełnomocnictwa, do ich złożenia, uzupełnienia lub poprawienia lub do udzielenia wyjaśnień w wyznaczonym terminie, chyba, że pomimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu lub konieczne byłoby unieważnienie postępowania.
8) Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania wezwać Wykonawców do złożenia wszystkich lub niektórych oświadczeń i dokumentów potwierdzających, że nie podlegają wykluczeniu oraz spełniają warunki udziału w postepowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów.
9) Zamawiający nie przewiduje zwołania zebrania Wykonawców.

ROZDZIAŁ IX. OPIS SPOSOBU PRZYGOTOWANIA OFERT INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

1. **INFORMACJE OGÓLNE:**
   1) Niniejsze postępowanie prowadzone jest zgodnie z art. 10a ust. 1 ustawy Pzp przy użyciu środków komunikacji elektronicznej.
   2) Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.
   3) Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z miniPortalu oraz Regulaminie ePUAP.
   4) Wykonawca biorący udział w niniejszym postępowaniu w formularzu oferty oświadcza, że zapoznał się oraz akceptuje warunki i zasady zawarte w Instrukcji użytkownika systemu miniPortal, Regulaminie korzystania z miniPortalu oraz Regulaminie Elektronicznej Platformy Usług Administracji Publicznej (ePUAP.).
   5) Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty lub wniosku oraz do komunikacji wynosi 150 MB.
   6) Za datę przekazania oferty, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP.
   7) W przypadku dokumentów składanych za pomocą poczty elektronicznej, za datę ich
   8) Identyfikator postępowania i klucz publiczny dla danego postępowania o udzielenie zamówienia dostępne są na Liście wszystkich postępowań na miniPortalu oraz stanowi Załącznik do niniejszej SIWZ.

2. **OPIS SPOSOBU SPORZĄDZANIA I INFORMACJE DOTYCZĄCE SKŁADANIA OFERT:**
   1) **Oferty wraz z wymaganymi załącznikami** w niniejszym postępowaniu (wraz z ewentualnymi zmianami lub wycofaniem w rozumieniu art. 84 ust. 1 ustawy Pzp) **składać należy wyłącznie przy użyciu miniPortalu** (https://miniportal.uzp.gov.pl/, ePUAPu https://epuap.gov.pl/wps/portal), adres skrytki Zamawiającego: GCIGdansk/SkrytkaESP,
   2) Wykonawca składa ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Klucz publiczny niezbędny do zaszyfrowania oferty przez Wykonawcę jest dostępny dla Wykonawców na

miniPortalu. W formularzu oferty Wykonawca zobowiązany jest podać adres skrzynki ePUAP, na którym prowadzona będzie korespondencja związana z postępowaniem.

3) Oferta powinna być sporządzona w języku polskim, z zachowaniem postaci elektronicznej w formacie danych doc., docx., rtf, xps, odt, pdf **i podpisana kwalifikowanym podpisem elektronicznym (przez osobę/y uprawnioną/e do tej czynności).** Sposób złożenia oferty w tym zaszyfrowania oferty opisany został w Regulaminie korzystania z miniPortal. Ofertę należy złożyć w formie dokumentu elektronicznego.
4) Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa" a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP). Szczegółowe informacje w zakresie tajemnicy przedsiębiorstwa zawiera ust. 6 niniejszego rozdziału.
5) **Do oferty należy dołączyć Jednolity Europejski Dokument Zamówienia w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).**
6) Wykonawca może złożyć tylko jedną ofertę. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę. W przypadku gdy postępowanie zostało podzielone na części (zadania), Wykonawca może złożyć jedną ofertę na daną część postępowania. Złożenie większej liczby ofert (w danej części postępowania) przez tego samego Wykonawcę, spowoduje odrzucenie wszystkich ofert złożonych przez tego Wykonawcę w danej części postępowania.
7) Oferta musi być sporządzona zgodnie z wymogami niniejszej SIWZ i ustawy Pzp. Treść oferty musi odpowiadać treści SIWZ. Oferta musi zawierać następujące oświadczenia i dokumenty wymienione w pierwszej części tabeli (część druga dotyczy dokumentów składanych w toku badania i oceny ofert):

Dokument / oświadczenie	**Numer załącznika**
I.	
W TERMINIE SKLADANIA OFERT, W SPOSÓB OKREŚLONY W ROZDZIALE IX. SIWZ W PUNKCIE DOTYCZĄCYM SKŁADANIA OFERT	
Formularz oferty (oryginał w formie dokumentu elektronicznego)	Załącznik nr 1
Formularz cenowy (oryginał w formie dokumentu elektronicznego)	Załącznik nr 2
JEDZ (oryginał w formie dokumentu elektronicznego)	Załącznik nr 3
Opcjonalnie: pełnomocnictwo *(oryginał – w formie dokumentu elektronicznego lub elektronicznej kopii poświadczonej notarialnie).* *Jeśli występuje pełnomocnik, pełnomocnictwo dla osoby reprezentującej w niniejszym postępowaniu Wykonawcę lub pełnomocnictwo do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia (w przypadku wspólnego ubiegania się o zamówienie – zgodnie z art. 23 ust. 2 ustawy).*	-
Opcjonalnie: zobowiązanie innego podmiotu *Opcjonalnie - pisemne zobowiązania podmiotów oddających do dyspozycji Wykonawcy niezbędne zasoby na potrzeby realizacji zamówienia (w formie oryginału, w formie dokumentu elektronicznego), o ile taka okoliczność wystąpiła w postępowaniu.*	-
Opcjonalnie: w przypadku Wykonawcy oferującego Produkty równoważne *Wykonawca wraz z ofertą składa dokumenty potwierdzające, że oferowane przez niego Produkty spełniają wymagania w zakresie równoważności opisane w SIWZ.*	-
Opcjonalnie: gwarancja lub poręczenie *Do oferty należy dołączyć* ***oryginał gwarancji lub poręczenia****, w przypadku jeśli wadium wnoszone jest w innej formie niż pieniądz (w formie elektronicznego dokumentu).*	-
II.	
DOKUMNETY I OŚWIADCZENIA – SKŁADANE W TOKU POSTĘPOWANIA W ORYGINALE W POSTACI DOKUMENTU ELEKTRONICZNEGO LUB ELEKTRONICZEJ KOPII DOKUMENTU.	

8) Formularz oferty, oświadczenia Wykonawcy oraz zobowiązania innych podmiotów, o których mowa w art. 22a ust. 2 ustawy Pzp należy złożyć w formie oryginałów.
9) Wymagane pełnomocnictwa należy złożyć w formie oryginałów lub w kopii poświadczonej przez notariusza.
10) Pozostałe dokumenty (inne niż wymienione w pkt 8 i 9), mogą być złożone w formie oryginałów lub poświadczonych za zgodność z oryginałem elektronicznych kopii. Czynności poświadczenia za zgodność z oryginałem dokonuje Wykonawca albo inny podmiot albo Wykonawca wspólnie ubiegający się o udzielenie zamówienia publicznego – odpowiednio, w zakresie dokumentów, które każdego z nich dotyczą. W przypadku przekazywania przez Wykonawcę elektronicznej kopii dokumentu, podpisanie jej przez upoważnioną osobę kwalifikowanym podpisem elektronicznym jest równoznaczne z poświadczeniem elektronicznej kopii dokumentu za zgodność z oryginałem. Jeżeli do reprezentowania Wykonawcy upoważnione są łącznie dwie lub więcej osób, kopie dokumentów muszą być potwierdzone za zgodność z oryginałem przez wszystkie te osoby.
11) W przypadku podpisania oferty oraz poświadczenia za zgodność z oryginałem kopii dokumentów przez osobę niewymienioną w dokumencie rejestracyjnym (ewidencyjnym) Wykonawcy, należy do oferty dołączyć stosowne pełnomocnictwo w oryginale lub kopii poświadczonej notarialnie.
12) Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
13) Wykonawca poniesie koszty związane z przygotowaniem i złożeniem oferty.
14) **Zamawiający nie ponosi odpowiedzialności za zdarzenia wynikające z niewłaściwego zaszyfrowania ofert lub niewłaściwego złożenia ofert.**
15) **Wszystkie dokumenty lub oświadczenia, o których mowa w niniejszej SIWZ lub ogłoszeniu o zamówieniu, składane są w oryginale – w postaci dokumentu elektronicznego lub elektronicznej kopii dokumentu poświadczonej za zgodność z oryginałem. Poświadczenie kopii za zgodność z oryginałem odbywa się opatrując dany dokument kwalifikowanym podpisem elektronicznym.**

3. **KOMUNIKACJA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCAMI:**
   1) W niniejszym postępowaniu o udzielenie zamówienia publicznego komunikacja między Zamawiającym a Wykonawcami **w szczególności składanie oświadczeń, wniosków (innych niż wymienione powyżej w ust. 3), zawiadomień oraz przekazywanie informacji odbywa się elektronicznie, za pośrednictwem:**
      a. poczty elektronicznej – na adres e-mail: zp@gdansk.gda.pl (preferowana forma), lub
      b. dedykowanego formularza dostępnego na ePUAP oraz udostępnionego przez miniPortal (Formularz do komunikacji).
   2) We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia (BZP, TED lub ID postępowania). W korespondencji kierowanej do Zamawiającego Wykonawca winien posługiwać się również numerem sprawy określonym w SIWZ.
   3) Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem Formularza do komunikacji jako załączniki. Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń za pomocą poczty elektronicznej, na wskazany w pkt 1 lit. a) adres email. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych oraz rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia.
   4) Zamawiający wyznacza do kontaktu z Wykonawcami Panią Katarzynę Basałaj, tel. 58 768 82 88, email: zp.@gdansk.gda.pl. Zamawiający nie będzie udzielał ustnie lub telefonicznie jakichkolwiek wyjaśnień treści SIWZ, odpowiedzi na pytania oraz konsultacji związanych z prowadzonym postępowaniem o udzielenie zamówienia publicznego.
   5) **W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia wszelka korespondencja prowadzona będzie wyłącznie z pełnomocnikiem.**

4. **WYJAŚNIENIA TREŚCI SIWZ.**
   1) Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ. Wykonawca w przypadku stwierdzenia konieczności wprowadzenia zmian lub modyfikacji w przedmiocie zamówienia zwraca się z wnioskiem do Zamawiającego w trybie określonym w art. 38 ustawy Pzp.
   2) Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa terminu składania ofert, Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na **6 dni** przed upływem terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu, o którym mowa powyżej, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
   3) Treść zapytań wraz z wyjaśnieniami zostanie przekazana Wykonawcom, którym Zamawiający przekazał SIWZ, bez ujawnienia źródła zapytania oraz zamieszczona na stronie internetowej, na której udostępniona jest SIWZ.
   4) Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SIWZ.
   5) W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert, zmienić treść niniejszej SIWZ. Dokonaną zmianę Zamawiający przekaże niezwłocznie wszystkim Wykonawcom, którym przekazano SIWZ oraz zamieści ją na stronie internetowej na której udostępniona jest SIWZ.
   6) Jeżeli w wyniku zmiany treści SIWZ nieprowadzącej do zmiany treści ogłoszenia o zamówieniu jest niezbędny dodatkowy czas na wprowadzenie zmian w ofertach, Zamawiający przedłuży termin składania ofert. O przedłużeniu terminu składania ofert Zamawiający niezwłocznie zawiadomi Wykonawców. Informację powyższą Zamawiający zamieści również na stronie na stronie internetowej na której udostępniona jest SIWZ.
   7) W przypadku rozbieżności pomiędzy treścią niniejszej SIWZ, a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.
   8) Oferta, której treść nie będzie odpowiadać treści SIWZ, z zastrzeżeniem art. 87 ust. 2 pkt 3 ustawy Pzp zostanie odrzucona (art. 89 ust. 1 pkt 2 ustawy Pzp). Wszelkie niejasności i wątpliwości dotyczące treści zapisów w SIWZ należy zatem wyjaśnić z Zamawiającym przed terminem składania ofert w trybie przewidzianym powyżej. Przepisy ustawy Pzp nie przewidują negocjacji warunków udzielenia zamówienia, w tym zapisów Istotnych Postanowień Umowy po terminie otwarcia ofert. Wykonawca składający ofertę w postępowaniu w pełni akceptuje warunki określone przez Zamawiającego w SIWZ wraz z załącznikami.

5. **ZMIANA TREŚCI OFERTY LUB WYCOFANIE OFERTY:**
   1) Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty dostępnego na ePUAP i udostępnionych również na miniPortalu. Sposób zmiany i wycofania oferty został opisany w Instrukcji użytkownika systemu dostępnej na miniPortalu.
   2) Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

6. **TAJEMNICA PRZEDSIĘBIORSTWA:**
   1) Zamawiający informuje, iż zgodnie z art. 8 w zw. z art. 96 ust. 3 ustawy Pzp oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.), jeśli Wykonawca w terminie składania ofert zastrzegł, że nie mogą one być udostępniane i jednocześnie wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
   2) Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli wykonawca, nie później niż w terminie składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy Pzp.

3) Wykonawca może zastrzec w ofercie stosownym oświadczeniem, iż Zamawiający nie będzie mógł ujawnić informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, tj. nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności,
4) **Wykonawca nie później niż w terminie składania ofert musi wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa,** strony oferty będące tajemnicą przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji, co, do których Wykonawca zastrzega, że nie mogą być one udostępniane innym uczestnikom postępowania.
5) Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.
6) Zastrzeżenie informacji, które nie stanowią tajemnicy przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji będzie traktowane, jako bezskuteczne i skutkować będzie zgodnie z uchwałą SN z 20 października 2005 (sygn. III CZP 74/05) ich odtajnieniem.
7) Zamawiający informuje, że w przypadku kiedy Wykonawca otrzyma od niego wezwanie w trybie art. 90 ustawy Pzp, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie zamawiający uzna za skuteczne wyłącznie w sytuacji kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa.

7. **PEŁNOMOCNICTWO:**
   1) Pełnomocnictwo do reprezentowania Wykonawcy / Wykonawców wspólnie ubiegających się o udzielenie zamówienia, powinno być dołączone do oferty.
   2) Pełnomocnictwo musi zawierać jego zakres i być udzielone przez osoby uprawnione do reprezentacji Wykonawcy. Pełnomocnictwo winno być podpisane kwalifikowanym podpisem elektronicznym.
   3) Pełnomocnictwo może być złożone w formie oryginału lub elektronicznej kopii potwierdzonej za zgodność z oryginałem przez notariusza.

ROZDZIAŁ X. WYMAGANIA DOTYCZĄCE WADIUM

1. Każdy Wykonawca zobowiązany jest zabezpieczyć swą ofertę wadium w wysokości: **40 000,00 zł.**
2. **Wadium może być wniesione w jednej lub kilku następujących formach:**
   1) pieniądzu (przelew bankowy),
   2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym,
   3) gwarancjach bankowych,
   4) gwarancjach ubezpieczeniowych,
   5) poręczeniach udzielanych przez podmioty, o których mowa w art. 6 b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (tekst jednolity Dz. U. z 2014 r. poz. 1804 oraz z 2015 r. poz. 978 i 1240).
3. **Dokument wadialny (poręczenie lub gwarancja) musi być sporządzony zgodnie z obowiązującym prawem, w formie oryginału (dokument elektroniczny) i zawierać następujące elementy:**
   1) nazwę oraz wskazanie siedziby: dającego zlecenie (Wykonawcy), beneficjenta gwarancji/poręczenia (dokument winien być wystawiony na **Gminę Miasta Gdańska, NIP 583-00-11-969 z siedzibą w Gdańsku (80-803) przy ul. Nowe Ogrody 8/12, w imieniu której działa Gdańskie Centrum Informatyczne z siedzibą w Gdańsku (80-601) przy ul. Prof. Witolda Andruszkiewicza 5),** oraz gwaranta/poręczyciela (banku, instytucji ubezpieczeniowej lub podmiotu poręczającego),
   2) określenie postępowania o udzielenie zamówienia publicznego, którego dotyczy,
   3) kwotę,
   4) termin ważności,

5) mieć formę oświadczenia bezwarunkowego płatnego na pierwsze pisemne żądanie Zamawiającego, bez pośrednictwa banku lub innej tego typu instytucji,
6) być nieodwołalny,
7) obejmować odpowiedzialność za wszystkie przypadki powodujące utratę wadium przez Wykonawcę, określone w art. 46 ust. 4a oraz ust. 5 ustawy Pzp,
8) a także obejmować cały okres związania ofertą, określony w SIWZ.

4. Wadium w pieniądzu należy wnieść przelewem na następujący rachunek **Gdańskiego Centrum Informatycznego 02 1240 1268 1111 0010 7864 3106** z dopiskiem: **„Wadium do przetargu: „Dostawa Produktów Microsoft lub Produktów równoważnych w ramach środowiska pracy grupowej - ZP/6/D/2019/K”.**
5. **Wniesienie wadium w pieniądzu za pomocą przelewu bankowego Zamawiający będzie uważał za skuteczne tylko wówczas, gdy bank prowadzący rachunek Zamawiającego potwierdzi, że otrzymał taki przelew przed upływem terminu składania ofert.**
6. **W przypadku wnoszenia wadium w innej formie niż w pieniądzu, wskazanej w ust. 1, należy do oferty dołączyć oryginał dokumentu w formie elektronicznej (opatrzony kwalifikowanym podpisem elektronicznym).**
7. Zaleca się, aby Wykonawca złożył wraz z ofertą potwierdzenie wniesienia wadium w pieniądzu, nie stanowi to jednak obowiązku.
8. Zamawiający dokona zwrotu wadium Wykonawcom zgodnie z art. 46 ust. 1 – 4 Ustawy Pzp
9. Zamawiający żąda ponownego wniesienia wadium przez Wykonawcę, któremu zwrócono wadium, jeżeli w wyniku rozstrzygnięcia odwołania jego oferta została wybrana jako najkorzystniejsza. Wykonawca wnosi wadium w terminie określonym przez Zamawiającego.
10. Wadium musi obejmować cały okres związania ofertą.
11. W ofercie należy wpisać nr konta, na który Zamawiający będzie mógł zwrócić wadium wpłacone w pieniądzu.
12. Zamawiający odrzuci ofertę jeżeli wadium nie zostało wniesione lub zostało wniesione w sposób nieprawidłowy.
13. Zamawiający zatrzyma wadium wraz z odsetkami, zgodnie z art. 46 ust. 4a oraz ust. 5 ustawy Pzp.

ROZDZIAŁ XI. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawcy składający ofertę będą nią związani **60 dni od upływu terminu składania ofert**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu na zasadach określonych w art. 85 ustawy Pzp.

ROZDZIAŁ XII. TERMIN SKŁADANIA I OTWARCIA OFERT

1. **Składanie ofert.**
   Oferty należy składać do dnia **23.04.2019 r. do godz. 9:00 w sposób określony w niniejszej SIWZ.**

2. **Otwarcie ofert.**
   1) Otwarcie ofert nastąpi w pok. nr 3/11 w **Gdańskim Centrum Informatycznym** ul. Prof. Witolda Andruszkiewicza 5, 80 – 601 Gdańsk (III piętro, budynek - Centrum Administracyjno-Usługowe KOGA), w dniu **23.04.2019 r. o godz. 13:00**
   2) Otwarcie ofert następuje poprzez użycie aplikacji do szyfrowania ofert dostępnej na miniPortalu i dokonywane jest poprzez odszyfrowanie i otwarcie ofert za pomocą klucza prywatnego.
   3) Otwarcie ofert jest jawne.
   4) Niezwłocznie po otwarciu ofert Zamawiający zamieści na stronie internetowej (w miejscu zamieszczenia SIWZ) informację z otwarcia ofert.

ROZDZIAŁ XIII. OPIS SPOSOBU OBLICZENIA CENY

1. Cenę należy obliczyć a następnie wpisać w wyznaczonym miejscu w druku formularza oferty stanowiącym Załącznik nr 1 do SIWZ.
2. Łączna cena ofertowa brutto (zawierająca podatek VAT) musi uwzględniać wszystkie czynniki cenotwórcze, wszelkie koszty niezbędne dla realizacji przedmiotu zamówienia – wynikające z treści SIWZ w tym szczegółowego opisu przedmiotu zamówienia, załącznika – Istotne Postanowienia Umowy jak i własnej wiedzy i doświadczenia.
3. Rozliczenia między Zamawiającym a wybranym Wykonawcą prowadzone będą w polskich złotych.
4. Ceny muszą być: podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (zasada zaokrąglenia – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
5. Cena oferty winna być wyrażona w złotych polskich (PLN).
6. Jeżeli w postępowaniu złożona będzie oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. W takim przypadku Wykonawca, składając ofertę, jest zobligowany poinformować Zamawiającego, że wybór jego oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę usługi, których świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
7. W przypadku złożenia przez Wykonawców dokumentów, w których jakiekolwiek kwoty podane zostały w walutach obcych, Zamawiający przeliczy te kwoty na PLN według średniego kursu Narodowego Banku Polskiego (dalej NBP), obowiązującego w dniu publikacji ogłoszenia o zamówieniu w Suplemencie do Dziennika Urzędowego Unii Europejskiej. Jeżeli w dniu publikacji ogłoszenia o zamówieniu NBP nie publikuje informacji o średnim kursie walut, Zamawiający dokona odpowiednich przeliczeń według średniego kursu z pierwszego kolejnego dnia, w którym NBP opublikuje w/w informacje.

ROZDZIAŁ XIV. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Oferty oceniane będą w oparciu o następujące kryteria (wskazane w tabeli, obowiązujące dla każdej części postępowania, dla zamówienia podstawowego oraz zamówienia objętego prawem opcji), którym Zamawiający przypisał następujące znaczenie:

1.	**Kryterium cenowe (cena brutto)**	**60%**
2.	**Inne kryteria:** **Termin płatności.** **Termin realizacji obowiązujący dla zamówienia objętego prawem opcji (dostawy Produktu).**	**40%**

1) <u>KRYTERIUM CENOWE: 60 % (maksymalna liczba punktów: 60)</u>
Ocena punktowa dokonana zostanie według poniższego wzoru:

$$\text{Liczba punktów przyznanych badanej ofercie} = \frac{\text{Najniższa cena wśród złożonych ofert (ofert ważnych, nie podlegających odrzuceniu)}}{\text{Cena badanej oferty}} \times 60 \text{ pkt.}$$

2) <u>INNE KRYTERIA: łącznie 40% (maksymalna liczba punktów: 40)</u>
Kryteria odnoszące się do przedmiotu zamówienia, ocena punktowa dokonana zostanie według poniższego podziału:

a. Termin płatności

Wariant do wyboru przez Wykonawcę	Termin płatności obowiązuje dla zamówienia podstawowego i zamówienia objętego prawem opcji.	Liczba punktów
1	**21 dni**	**0**
2.	**30 dni**	**20**

W przypadku gdy Wykonawca zaoferuje dłuższy termin płatności aniżeli określony jako najwyższy, Zamawiający nie przyzna dodatkowych punktów, lecz maksymalną liczbę punktów przewidzianą w tym kryterium.

b. Termin realizacji zamówienia objętego prawem opcji (liczony od dnia przesłania Oświadczenia Zamawiającego o skorzystaniu z zamówienia objętego prawem opcji, na zasadach określonych w IPU).

Wariant do wyboru przez Wykonawcę	Termin realizacji w ramach zamówienia objętego prawem opcji (dostawy)	Liczba punktów
1.	**7 dni roboczych od dnia przesłania Oświadczenia**	**0**
2.	**5 dni roboczych od dnia przesłania Oświadczenia**	**20**

W przypadku gdy Wykonawca zaoferuje krótszy termin realizacji aniżeli określony w wariancie 2, Zamawiający nie przyzna dodatkowych punktów, lecz maksymalną liczbę punktów przewidzianą w tym kryterium.

2. Punktacja przyznawana Wykonawcom w poszczególnych kryteriach, gdzie wymagane są obliczenia – będzie liczona z dokładnością do dwóch miejsc po przecinku. W przypadku, gdy Wykonawca wybierze jeden z wariantów, Zamawiający przyzna liczbę punktów adekwatnie do wybranej opcji. Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę. **Zamawiający po przeliczeniu punktów przyznanych badanej ofercie w każdym kryterium oceny ofert, dokona zsumowania punktów. Uzyskany wynik, będzie stanowił całkowitą liczbę punktów przyznanych badanej ofercie.**
3. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiadać będzie wszystkim wymaganiom przedstawionym w ustawie Pzp, oraz w SIWZ i zostanie oceniona jako najkorzystniejsza w oparciu o podane kryteria wyboru.
4. Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny lub kosztu i innych kryteriów oceny ofert Zamawiający spośród tych ofert wybiera ofertę z najniższą ceną lub najniższym kosztem, a jeżeli zostały złożone oferty o takiej samej cenie lub koszcie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych (w myśl art. 91 ust. 4 ustawy Pzp).

ROZDZIAŁ XV. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Zamawiający zawiadomi wszystkich uczestników niniejszego postępowania o udzielenie zamówienia publicznego o wyborze najkorzystniejszej oferty oraz zamieści stosowaną informację na stronie internetowej na której udostępnił SIWZ.
2. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.
3. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający może żądać przed zawarciem umowy przedstawienia umowy regulującej współpracę tych Wykonawców.
4. Zawarcie umowy nastąpi na podstawie Załącznika nr 9 do SIWZ– Istotne Postanowienia Umowy.
5. Postanowienia ustalone w załączniku Istotne Postanowienia Umowy nie podlegają negocjacjom.

6. W przypadku, gdy Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy, Zamawiający będzie mógł wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzenia ich ponownego badania i oceny chyba, że zachodzą przesłanki, o których mowa w art. 93 ust. 1 ustawy Pzp.

ROZDZIAŁ XVI. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ XVII. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, OGÓLNE WARUNKI UMOWY ALBO WZÓR UMOWY, JEŻELI ZAMAWIAJĄCY WYMAGA OD WYKONAWCY, ABY ZAWARŁ Z NIM UMOWĘ W SPRAWIE ZAMÓWIENIA PUBLICZNEGO NA TAKICH WARUNKACH

1. Istotne postanowienia umowy, stanowi Załącznik nr 9 do SIWZ.
2. Wykonawca winien zapoznać się z treścią Załącznika do SIWZ – istotne postanowienia umowy oraz w przypadku, gdy nie wnosi żadnych zastrzeżeń dotyczących postanowień i warunków, określonych w istotnych postanowieniach umowy, zaakceptować jego treść na formularzu „Oferta”.

ROZDZIAŁ XVIII. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

1. Każdemu Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy PZP przysługują środki ochrony prawnej przewidziane w dziale VI ustawy Pzp jak dla postępowań powyżej kwoty określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 ustawy Pzp.
2. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz SIWZ przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 ustawy Pzp.

ROZDZIAŁ XIX. ZAŁĄCZNIKI DO SIWZ

Załącznik nr 1	Formularz oferty.
Załącznik nr 2	Formularz cenowy.
Załącznik nr 3	JEDZ.
Załącznik nr 4	Oświadczenie / Lista podmiotów należących do tej samej grupy kapitałowej, o której mowa w /informacja o tym, że Wykonawca nie należy do grupy kapitałowej (dokument składany po otwarciu ofert na zasadach określonych w SIWZ).
Załącznik nr 5	Wykaz dostaw.
Załącznik nr 6	Oświadczenie Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne.
Załącznik nr 7	Oświadczenie Wykonawcy o braku orzeczenia wobec niego zakazu ubiegania się o zamówienie publiczne.
Załącznik nr 8	Opis przedmiotu zamówienia.
Załącznik nr 9	Istotne postanowienia umowy.

Załącznik nr 8 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

I. Informacje ogólne.

1. Przedmiotem zamówienia jest **dostawa Produktów Microsoft lub Produktów równoważnych w ramach środowiska pracy grupowej. Produkty należące do przedmiotu zamówienia:**
   1) **Licencje,**
   2) **Licencje subskrypcyjne (licencjonowane na Użytkownika),**
   3) **Usługi.**

2. **Harmonogram realizacji przedmiotu zamówienia:**

Lp./ Etap realizacji przedmiotu zamówienia (wiersze scalone)	Produkty (lub produkty równoważne do podanych poniżej)	Rodzaj produktu LS - Licencja subskrypcyjna, U – Usługa L – Licencja	Termin Dostawy Technicznej (prognozowany) Dla zamówienia objętego prawem opcji Dostawa Właściwa = Dostawa Techniczna	Termin Dostawy Właściwej (prognozowany)	Termin używania Produktu (w miesiącach liczony od Dostawy Właściwej) W przypadku zamówienia objętego prawem opcji podany termin jest maksymalnym terminem	Termin zakończenia używania Produktu liczony od daty dostawy właściwej (w przypadku zamówienia objętego prawem opcji – maksymalny termin)	Liczba Produktów (sztuk) zgodnie z okresem wskazanym w kolumnie nr 6
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
ZAMÓWIENIE PODSTAWOWE:							
ETAP 1.							
1.	Microsoft Office 365 E3	LS	15.06.2019 r.	30.06.2019 r.	**36**	30.06.2022 r.	**585**
2.	Microsoft Office 365 E1	LS	15.06.2019 r.	30.06.2019 r.	**36**	30.06.2022 r.	**950**
3.	Microsoft Project Online Professional	LS	15.06.2019 r.	30.06.2019 r.	**36**	30.06.2022 r.	**7**
4.	Microsoft Visio Onlnine Plan 2	LS	15.06.2019 r.	30.06.2019 r.	**36**	30.06.2022 r.	**4**
ETAP 2.							
1.	Microsoft Exchange Online Archiving	LS	15.09.2019 r.	30.09.2019 r.	**33**	30.06.2022 r.	**950**
ETAP 3.							
1.	Microsoft Office 365 E3	LS	15.12.2019 r.	31.12.2019 r.	**30**	30.06.2022 r.	**20**
2.	Microsoft Office 365 E1	LS	15.12.2019 r.	31.12.2019 r.	**30**	30.06.2022 r.	**80**
3.	Microsoft Exchange Online Archiving	LS	15.12.2019 r.	31.12.2019 r.	**30**	30.06.2022 r.	**80**
ZAMÓWIENIE OBJĘTE PRAWEM OPCJI:							
ETAP 4.							
1.	Microsoft Office 365 E3	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1067**
2.	Microsoft Office 365 E1	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1068**
3.	Microsoft Exchange Online Archiving	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**534**
4.	Microsoft Office 365 E5	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
5.	Microsoft Exchange Online Plan 1	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
6.	Microsoft Exchange Online Plan 2	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**

7.	Microsoft Project Online Essentials	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
8.	Microsoft Project Online Professional	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
9.	Microsoft Project Online Premium	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
10.	Microsoft Visio Onlnine Plan 1	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
11.	Microsoft Visio Onlnine Plan 2	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
12.	Microsoft Azure Information Protection Premium P1	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
13.	Microsoft Azure Information Protection Premium P2	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
14.	Microsoft Office 365 Advanced Treat Protection	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
15.	Microsoft Office 365 Data Loss Prevention	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
16.	Microsoft Enterprise Mobility + Security	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
17.	Microsoft Azure Multifactor Authentication	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
18.	Microsoft 365 E3	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**20**
19.	Microsoft 365 E5	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
20.	Office 365 E3 z Office 365 E1 step up	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**534**
21.	Office 365 E5 z Office 365 E1 step up	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
22.	Office 365 E5 z Office 365 E3 step up	LS	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
23.	Microsoft Azure Monetary Commitment	U	-	30.06.2019 r.	**36**	30.06.2022 r.	**1**
24.	Microsoft Premier Professional Enterprice Service	U	-	30.06.2019 r.	**12**	Po 12 miesiącach	**1**
25.	Microsoft Premier Professional Enterprice Service AddOn	U	-	30.06.2019 r.	**12**	Po 12 miesiącach	**1**
26.	Office Std Dev SL	L	-	30.06.2019 r.	bezterminowo	Nie dotyczy	**534**

3. **Oferowane Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).**
4. **W przypadku zaoferowania przez Wykonawcę Produktów Microsoft, Zamawiający wymaga aby dostawy tychże Produktów odbyły się na warunkach zagwarantowanych dla jednostek finansów publicznych w umowach ramowych podpisanych pomiędzy Producentem oprogramowania, a Ministerstwem Cyfryzacji.**
5. **Zawarte w Opisie przedmiotu zamówienia wymagania i zobowiązania Wykonawcy – o ile nie zastosowano wyłączenia – dotyczą zarówno Wykonawcy, który dostarczy Produkty Microsoft, jak i Wykonawcy, który dostarczy Produkty równoważne**.

6. Zamawiający wymaga, aby Wykonawca posiadał w momencie składania oferty oraz przez cały okres obowiązywania Umowy w sprawie zamówienia publicznego status Licensing Solution Provider (LSP), za wyjątkiem Wykonawcy oferującego Produkty równoważne.
7. Wszystkie Produkty wymienione w niniejszym opisie przedmiotu zamówienia muszą pochodzić bezpośrednio od Producenta lub z oficjalnych i autoryzowanych przez Producenta kanałów dystrybucyjnych. Zamawiający wymaga, aby Wykonawca posiadał kwalifikacje i uprawnienia wymagane do prawidłowej realizacji przedmiotu zamówienia.
8. Zamawiający wymaga, aby Wykonawca dostarczył najnowsze wersje Produktów o ile opis przedmiot zamówienia nie stanowi inaczej.
9. Poziom dostępności Licencji Subskrypcyjnych i nie może być mniejszy niż 99,9% w skali miesiąca.
10. **Zobowiązania Wykonawcy zostały określone w Załączniku nr 9 do SIWZ – Istotne postanowienia umowy (IPU).**
11. **Wykonawca dostarczy Zamawiającemu wszelkie dane niezbędne do prawidłowej instalacji i uruchomienia Produktów, zgodnie z zapisami IPU.**
12. **Zasady korzystania z Produktów:**
    1) w przypadku Produktów Microsoft ogólne zasady zakupu Produktów muszą być zgodne z postanowieniami umów ramowych MBSA lub MPSA (zwane w IPU Umowami ramowymi);
    2) W przypadku Licencji Subskrypcyjnych Zamawiający wymaga świadczenia usługi wsparcia technicznego przez cały okres używania Licencji Subskrypcyjnych. Usługa wsparcia technicznego świadczona będzie przez Producenta (zarówno w przypadku Produktów Microsoft jak i Produktów równoważnych),
    3) W przypadku Licencji – Zamawiający wymaga świadczenia usługi wsparcia technicznego przez co najmniej 60 miesięcy od daty dostawy licencji lub daty zakończenia wsparcia ogłoszonego przez producenta. Usługa wsparcia technicznego świadczona będzie przez Producenta (zarówno w przypadku Produktów Microsoft jak i Produktów równoważnych),
    4) W przypadku Licencji - licencjonowanie musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez Producenta uaktualnień, poprawek krytycznych i opcjonalnych w okresie co najmniej 60 miesięcy od dnia dostawy Licencji lub daty zakończenia wsparcia ogłoszonego przez producenta,
    5) dostarczane Produkty muszą posiadać zbiorcze i indywidualne dokumenty pozwalające na stwierdzenie legalności zakupionych Produktów dla celów inwentaryzacyjnych i audytowych; dokumenty takie Wykonawca będzie wystawiał na żądanie Zamawiającego,
    6) Zamawiający dopuszcza oferowanie Produktów o szerszym zakresie funkcjonalnym od wymaganego,
    7) **dostarczane Produkty i świadczone usługi należące do przedmiotu zamówienia muszą spełniać postanowienia wynikające Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.**

13. Zakres funkcjonalności Platformy do zarządzania produktami:
    1) Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach **Platformy.**
    2) Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa,
    3) Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla Licencji Subskrypcyjnych,
    4) Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
    5) Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi Platformowej**.**
    6) Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
    7) Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione".
    8) Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN)
    9) Wbudowane w Platformę mechanizmy zabezpieczające przez atakami DDoS,

10) Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km.
11) Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego.
12) Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
13) Gwarancję usunięcia danych Zamawiającego z Platformy po zakończeniu umowy.
14) Gwarancję braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji **Wykonawcy Platformy.**

14. Z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianych Produktów oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga oferty zawierającej Produkty, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego oraz jednolitych mechanizmów wykorzystania tożsamości cyfrowej.
15. Jeżeli nowa wersja Produktu zawierać będzie bardziej restrykcyjne prawa do używania niż wersja, która była aktualna na dzień złożenia oferty, te bardziej restrykcyjne prawa do używania nie będą miały zastosowania do korzystania z tego Produktu przez Zamawiającego.

16. **Wymagania szczególne - licencje:**
    1) Licencje muszą pozwalać na swobodne przenoszenie pomiędzy komputerami (np. w przypadku wymiany sprzętu);
    2) zakupione Licencje muszą być bezterminowe i posiadać wymagane klucze aktywacyjne;
    3) Licencje muszą pozwalać na udzielanie licencji dla jednostek organizacyjnych GMG + UM.
    4) Dla Licencji wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego Produktu i korzystania z kopii zamiennych (możliwość kopiowania Produktu na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji grupowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych;

17. **Wymagania szczególne dla subskrypcji licencyjnych:**
    1) w przypadku Subskrypcji – Zamawiający będzie korzystał z Subskrypcji przez czas określony w SIWZ;
    2) Subskrypcje będą udzielane na użytkownika.

18. **W przypadku zaoferowania przez Wykonawcę Produktów równoważnych, Zamawiający wymaga, aby oferowane Produkty spełniały dodatkowo niżej wymienione wymagania:**
    1) musi być możliwa implementacja Produktów (Licencje i Subskrypcje) na istniejących konfiguracjach środowiska produkcyjnego i testowego;
    2) równoważny Produkt musi bez zakłóceń współpracować z posiadaną przez Zamawiającego (i jednostki Gminy Miasta Gdańsk i Urzędu Miejskiego w Gdańsku) infrastrukturą sprzętową oraz wykorzystywanym oprogramowaniem i systemami, do których należą: serwery, laptopy, komputery stacjonarne, urządzenia drukujące, urządzenia sieciowe, systemy Windows, oprogramowanie Microsoft (SharePoint, Project Server), środowisko wirtualizacyjne VmWare. Na Wykonawcy oferującym Produkty równoważne spoczywa odpowiedzialność w zakresie prawidłowego działania zaoferowanych Produktów w środowisku pracy użytkowników Produktów po stronie Zamawiającego (w tym jednistek Gminy Miasta Gdańska i Urzędu Miejskiego w Gdańsku);
    3) Wykonawca musi zapewnić warunki i zakres usługi wsparcia Producenta dla Produktów równoważnych nie gorsze niż usługa określona dla odpowiedniego Produktu Producenta Microsoft;
    4) Warunki Licencji w każdym aspekcie licencjonowania nie mogą być gorsze niż dla licencji Producenta Microsoft;
    5) Wykonawca musi wykazać, że funkcjonalność każdego Produktu równoważnego nie jest gorsza od funkcjonalności odpowiedniego Produktu Producenta Microsoft;

6) 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;
7) Wykonawca musi zapewnić, że warunki i zakres usługi asysty wsparcie technicznego dla Produktów równoważnych nie są gorsze, niż usługi oferowane przez Producenta Microsoft;
8) 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;
9) Wykonawca zobowiązany jest pokryć koszty zmiany w zakresie Produktów i rozwiązań Microsoft na Produkty i rozwiązania równoważne, konieczne do właściwego działania środowiska sprzętowo- programowego Zamawiającego, Urzędu Miejskiego w Gdańsku oraz jednostek organizacyjnych Gminy Miasta Gdańska, będących jednostkami budżetowymi (Produkty będą również używane przez członków Rady Miasta Gdańska, dla której obsługę zapewnia Urząd Gminy Miasta Gdańska), oraz przeszkolenia personelu Zamawiającego, Urzędu Miejskiego w Gdańsku oraz jednostek organizacyjnych Gminy Miasta Gdańska jednostek należących do Gminy Miasta Gdańska (a także Rady Miasta Gdańska), o ile wystąpi taka konieczność;
10) Wykonawca zobowiązany jest przywrócić sprawne działanie infrastruktury sprzętowo-programowej Zamawiającego i jednostek organizacyjnych Gminy Miasta Gdańsk i Urzędu Miejskiego w Gdańsku 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 i w jednostkach Gminy Miasta Gdańsk i Urzędu Miejskiego w Gdańsku lub spowoduje zakłócenia w funkcjonowaniu pracy tego środowiska sprzętowo-programowego.

19. Zamawiający ze względu na koszty ewentualnej zmiany w zakresie rozwiązań Producenta Microsoft na Produkty równoważne, wymaga, aby Produkty równoważne pochodziły od jednego Producenta i umożliwiały wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania i monitorowania.

II. Informacje dotyczące produktów równoważnych - warunki równoważności produktów.

Microsoft Office 365 E1 lub równoważna **Subskrypcja pakietu usług hostowanych typ I - subskrypcja na użytkownika**

Subskrypcja pakietu 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 usługi hostowanej:

1. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę zarządzania tożsamością użytkowników.
2. Wbudowana usługa zarządzania tożsamością użytkowników musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
3. Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup.
4. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
5. Ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day.
6. Gwarantowana dostępność usług platformy na poziomie 99,9%,

7. Zastosowanie w Platformie powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy, w szczególności:
   - ISO 27001, ISO 27017, ISO 27018
   - SOC 2 lub 3
   - Open Authentication Standard – OAuth
8. Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy.
9. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z RODO.
10. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
11. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
12. 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".
13. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
14. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
15. Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km.
16. 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 ma zostać wyłączone a dane Zamawiającego usunięte.
17. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
18. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
19. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
20. 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.
21. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
22. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.
23. Zobowiązania umowne potwierdzające zgodność z rozp. RODO i potwierdzające rolę operatora usługi jako współprzetwarzającego dane,
24. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
25. Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.
26. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy Platformy.

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:

- Posiadanego oprogramowania Outlook (2010, 2013 i 2016),
- Przeglądarki (Web Access),
- Urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 30 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa najnowszych funkcji Outlook 2013 i 2016, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla 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:

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, 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.

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.
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 Internet Explorer, Apple Safari i Mozilla Firefox.

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

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych,
2. Zarządzanie strukturą portalu i treściami www,
3. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
4. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej,
5. Tworzenie repozytoriów wzorów dokumentów,
6. Tworzenie repozytoriów dokumentów,
7. Wspólną, bezpieczną pracę nad dokumentami,
8. Wersjonowanie dokumentów (dla wersji roboczych),
9. Organizację pracy grupowej,
10. Wyszukiwanie treści,
11. Dostęp do danych w relacyjnych bazach danych,
12. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

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

1. Interfejs użytkownika:
   - 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).
   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 ASP.NET, Apache, C#, Java i PHP,
   c. Możliwość osadzania elementów iFrame w polach HTML na stronie.
3. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
   a. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili
   b. Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów
   c. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili
   d. Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego
   e. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services

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 2010 i 2016z 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 zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
j. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

6. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   a. Przygotowywanie prezentacji multimedialnych, które będą:
   b. Prezentowanie przy użyciu projektora multimedialnego
   c. Drukowanie w formacie umożliwiającym robienie notatek
   d. Zapisanie jako prezentacja tylko do odczytu.
   e. Nagrywanie narracji i dołączanie jej do prezentacji
   f. Opatrywanie slajdów notatkami dla prezentera
   g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
   h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
   i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
   j. Możliwość tworzenia animacji obiektów i całych slajdów
   k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
   l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.

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

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

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

1. Wymianę informacji z możliwością wyboru i zmiany dostępnego kanału komunikacji, tj. wiadomości tekstowych (chat), rozmowy (przekazywanie dźwięku), wideo rozmowy (przekazywanie dźwięku i obrazu), współdzielenie lokalnych pulpitów w systemach Windows oraz współdzielenie dokumentów z możliwością przejmowania kontroli i edycji przez uprawnionych uczestników.
2. Kontakt poprzez wymienione kanały w modelu jeden do jednego, jeden do wielu, telekonferencji (kontakt interakcyjny wielu osób) oraz udostępniania dźwięku i obrazu dla wielu osób w sieci intranet lub internet.
3. Możliwość oceny jakości komunikacji głosowej i wideo.
4. Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze katalogowej oraz definiowania opisów użytkowników zewnętrznych w tym użytkowników wybranych bezpłatnych komunikatorów i użytkowników sieci telefonii przewodowej i komórkowej.
5. Dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub specjalizowanych urządzeń stacjonarnych typu telefon IP, kamera dookólna czy duże monitory lub projektory.
6. Dostępny kliencki sprzęt peryferyjny różnych producentów posiadający potwierdzenie zgodności z SKW przez producenta SKW.
7. Dostępność informacji o statusie dostępności użytkowników na liście adresowej (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności, w tym składowanych w usłudze katalogowej.

8. Możliwość grupowania kontaktów w komunikacji tekstowej z możliwością konwersacji typu jeden-do-jednego, jeden-do-wielu i możliwością rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat.
9. Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.
10. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.
11. Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
12. Możliwość nagrywania telekonferencji przez uczestników.
13. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
14. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
15. Wbudowana funkcjonalność mostka konferencyjnego MCU.
16. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
17. Kodowanie video H.264,
18. Wsparcie dla adresacji IPv4 i IPv6,
19. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
20. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników,
21. Możliwość szyfrowania połączeń.
22. Dostępność uczestniczenia w telekonferencjach poprzez przeglądarkę dla użytkowników z poza organizacji, zaproszonych do udziału w telekonferencji z funkcjami:
    a. Dołączania do telekonferencji,
    b. Szczegółowej listy uczestników
    c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
    d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
    e. Dostępu do udostępnianych plików,
    f. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji,
23. Dostępność aplikacji klienckiej usługi SKW (komunikatora) z funkcjonalnością:
    a. Listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielania grup kontaktów typu ulubione lub ostatnie.
    b. Historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
    c. Wsparcia telekonferencji:
        - Dołączania do telekonferencji,
        - Szczegółowej listy uczestników,
        - Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,
        - Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
        - Głosowania,
        - Udostępniania plików i pulpitów,
        - Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,
    d. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
    e. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

Wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji SKW z wybranymi systemami poczty elektronicznej i portali intranet/internet oraz usługą katalogową Active Directory.

Wynikiem takiej integracji mają być następujące funkcje i cechy systemu opartego o SKW dostępne dla użytkowników posiadających odpowiednie uprawnienia licencyjne i nadane przez administratorów:

1. Wykorzystanie domenowego mechanizmu uwierzytelnienia w oparciu o usługę katalogową, jej profile użytkowników i ich grup oraz realizację fizyczną pojedynczego logowania (single sign-on) dla uprawnionego dostępu do usług SKW.
2. Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).

3. Współdziałanie mechanizmów SKW z pocztą głosowa, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:
    a. Uruchamiania funkcji komunikacyjnych SKW z wybranych interfejsów klienta poczty elektronicznej, składników pakietu biurowego czy portalu,
    b. Dostępności w tych interfejsach danych o statusie obecności innych użytkowników (np. w nagłówkach poczty elektronicznej, czy listach użytkowników portalu.
    c. Możliwość planowania rozmów czy telekonferencji bezpośrednio poprzez zaproszenia w kalendarzu klienta poczty elektronicznej, generujące link do spotkania on-line.

Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 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.

Microsoft Office 365 E3 lub równoważna **Subskrypcja pakietu usług hostowanych typ II - subskrypcja na użytkownika**

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

1. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę zarządzania tożsamością użytkowników.
2. Wbudowana usługa zarządzania tożsamością użytkowników musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
3. Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup.
4. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
5. Ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day.
6. Gwarantowana dostępność usług platformy na poziomie 99,9%,
7. Zastosowanie w Platformie powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy, w szczególności:
    - ISO 27001, ISO 27017, ISO 27018
    - SOC 2 lub SOC 3
    - Open Authentication Standard – OAuth
8. Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy.
9. 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.
10. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
11. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
12. Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
13. 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".
14. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
15. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,

16. Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km.
17. 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.
18. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
19. Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich.
20. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
21. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
22. 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.
23. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
24. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.
25. Zobowiązania umowne potwierdzające zgodność z rozp. RODO i potwierdzające rolę operatora usługi jako współprzetwarzającego 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.
28. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy Platformy.

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:

- Posiadanego oprogramowania Outlook (2010, 2013 i 2016),
- Przeglądarki (Web Access),
- Urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 30 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa najnowszych funkcji Outlook 2013 i 2016, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla 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:

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 Internet Explorer, Apple Safari i Mozilla Firefox.

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

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych,
2. Zarządzanie strukturą portalu i treściami www,
3. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
4. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej,
5. Tworzenie repozytoriów wzorów dokumentów,
6. Tworzenie repozytoriów dokumentów,
7. Wspólną, bezpieczną pracę nad dokumentami,
8. Wersjonowanie dokumentów (dla wersji roboczych),
9. Organizację pracy grupowej,
10. Wyszukiwanie treści,
11. Dostęp do danych w relacyjnych bazach danych,
12. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

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

1. Interfejs użytkownika:
   a. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
   b. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
   c. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
   d. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
2. Projektowanie stron
   a. Wbudowane intuicyjne narzędzia projektowania wyglądu stron,

   b. Wsparcie dla ASP.NET, Apache, C#, Java i PHP,
   c. Możliwość osadzania elementów iFrame w polach HTML na stronie.
3. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
   a. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili
   b. Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów
   c. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili
   d. Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego
   e. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services
   f. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

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

1. Wymagania odnośnie interfejsu użytkownika:
   a. Pełna polska wersja językowa interfejsu użytkownika,
   b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych
2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
   a. posiada kompletny i publicznie dostępny opis formatu,
   b. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
3. Pakiet biurowy on-line musi zawierać:
   a. Edytor tekstów
   b. Arkusz kalkulacyjny
   c. Narzędzie do przygotowywania i prowadzenia prezentacji
   d. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.
4. Edytor tekstów musi umożliwiać:
   a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
   b. Wstawianie oraz formatowanie tabel
   c. Wstawianie oraz formatowanie obiektów graficznych
   d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego
   e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
   f. Automatyczne tworzenie spisów treści
   g. Formatowanie nagłówków i stopek stron
   h. Sprawdzanie pisowni w języku polskim
   i. Śledzenie zmian wprowadzonych przez użytkowników
   j. Określenie układu strony (pionowa/pozioma)
   k. Wydruk dokumentów
   l. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010 i 2016z zapewnieniem konwersji wszystkich elementów i atrybutów dokumentu
   m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
5. Arkusz kalkulacyjny musi umożliwiać:
   a. Tworzenie raportów tabelarycznych
   b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
   c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.

d. Wyszukiwanie i zamianę danych
e. Wykonywanie analiz danych przy użyciu formatowania warunkowego
f. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
g. Formatowanie czasu, daty i wartości finansowych z polskim formatem
h. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
i. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
j. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

6. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   a. Przygotowywanie prezentacji multimedialnych, 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. Zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.

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

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

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

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

9. Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.
10. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.
11. Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
12. Możliwość nagrywania telekonferencji przez uczestników.
13. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
14. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
15. Wbudowana funkcjonalność mostka konferencyjnego MCU.
16. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
17. Kodowanie video H.264,
18. Wsparcie dla adresacji IPv4 i IPv6,
19. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
20. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników,
21. Możliwość szyfrowania połączeń.
22. Dostępność uczestniczenia w telekonferencjach poprzez przeglądarkę dla użytkowników z poza organizacji, zaproszonych do udziału w telekonferencji z funkcjami:
    a. Dołączania do telekonferencji,
    b. Szczegółowej listy uczestników
    c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
    d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
    e. Dostępu do udostępnianych plików,
    f. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji,
23. Dostępność aplikacji klienckiej usługi SKW (komunikatora) z funkcjonalnością:
    a. Listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielania grup kontaktów typu ulubione lub ostatnie.
    b. Historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
    c. Wsparcia telekonferencji:
    f. Dołączania do telekonferencji,
    g. Szczegółowej listy uczestników,
    h. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,
    i. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
    j. Głosowania,
    k. Udostępniania plików i pulpitów,
    l. Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,
    24. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
    25. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

Wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji SKW z wybranymi systemami poczty elektronicznej i portali intranet/internet oraz usługą katalogową Active Directory.

Wynikiem takiej integracji mają być następujące funkcje i cechy systemu opartego o SKW dostępne dla użytkowników posiadających odpowiednie uprawnienia licencyjne i nadane przez administratorów:

1. Wykorzystanie domenowego mechanizmu uwierzytelnienia w oparciu o usługę katalogową, jej profile użytkowników i ich grup oraz realizację fizyczną pojedynczego logowania (single sign-on) dla uprawnionego dostępu do usług SKW.
2. Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).
3. Współdziałanie mechanizmów SKW z pocztą głosowa, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:

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

Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 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.

Subskrypcja pakietu biurowego
Usługa hostowana on-line musi zawierać subskrypcję pakietu biurowego spełniającego następujące wymagania:
Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit
2. Wymagania odnośnie interfejsu użytkownika:
   a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
   b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
   c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
3. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w 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,
5. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
6. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
7. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
8. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
9. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a. Edytor tekstów
   b. Arkusz kalkulacyjny
   c. Narzędzie do przygotowywania i prowadzenia prezentacji
   d. Narzędzie do tworzenia drukowanych materiałów informacyjnych
   e. Narzędzie do tworzenia i pracy z lokalną bazą danych
   f. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
   g. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
   h. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.

10. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c. Wstawianie oraz formatowanie tabel.
    d. Wstawianie oraz formatowanie obiektów graficznych.
    e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    g. Automatyczne tworzenie spisów treści.
    h. Formatowanie nagłówków i stopek stron.
    i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
    j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
    k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
    l. Określenie układu strony (pionowa/pozioma).
    m. Wydruk dokumentów.
    n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
    o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007, Microsoft Word 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
    p. Zapis i edycję plików w formacie PDF.
    q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
    r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco,
    s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.
11. Arkusz kalkulacyjny musi umożliwiać:
    a. Tworzenie raportów tabelarycznych
    b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
    c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
    d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
    e. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
    f. Wyszukiwanie i zamianę danych
    g. Wykonywanie analiz danych przy użyciu formatowania warunkowego
    h. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
    i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
    j. Formatowanie czasu, daty i wartości finansowych z polskim formatem
    k. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
    l. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
    m. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
    n. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
    o. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
12. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    a. Przygotowywanie prezentacji multimedialnych, które będą:
        i. 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 2007, MS PowerPoint 2010 i 2013.

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 7 lub wyższych oraz OSX 10 lub wyższych,
    d. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
    e. Możliwość obsługi tekstowych wiadomości błyskawicznych w modelu jeden do jeden i jeden do wielu.
    f. Możliwość komunikacji głosowej i video w modelu jeden do jeden i jeden do wielu.
    g. Obsługa telekonferencji SKW:
        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 specjalizowanych urządzeń peryferyjnych zgodnych z SKW.
    o. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
    p. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
        q. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Microsoft Office 365 E5 lub równoważna **Subskrypcja pakietu usług hostowanych typ III - subskrypcja na użytkownika**

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

1. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę LDAP.
2. Wbudowana usługa LDAP musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
3. Możliwość dodawania do 500 własnych nazw domenowych do usługi LDAP.
4. Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup.
5. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
6. Ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day.
7. 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.
8. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
9. Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich.
10. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
11. Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych w Usłudze własnością Zamawiającego.
12. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
13. 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.
14. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
15. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.

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:

- Posiadanego oprogramowania Outlook (2010, 2013 i 2016),
- Przeglądarki (Web Access),
- Urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 50 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,

- Obsługa najnowszych funkcji Outlook 2013, 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:

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 i SMS-ów.
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.

– 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.

- Wsparcie dla użytkowników mobilnych:

Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu opisanej w punkcie a). Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem
Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone
Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej
Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

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

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych,
2. Zarządzanie strukturą portalu i treściami www,
3. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
4. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej,
5. Tworzenie repozytoriów wzorów dokumentów,
6. Tworzenie repozytoriów dokumentów,
7. Wspólną, bezpieczną pracę nad dokumentami,
8. Wersjonowanie dokumentów (dla wersji roboczych),
9. Organizację pracy grupowej,
10. Wyszukiwanie treści,
11. Dostęp do danych w relacyjnych bazach danych,
12. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

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

1. Interfejs użytkownika:

- Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
- Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0

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.
   g. Wbudowane samoobsługowe narzędzia wyszukiwania, analizy i wizualizacji danych Typu BI wraz z raportowaniem.

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 2010 i 2016z zapewnieniem konwersji wszystkich elementów i atrybutów dokumentu
m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

5. Arkusz kalkulacyjny musi umożliwiać:
   a. Tworzenie raportów tabelarycznych
   b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
   c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d. Wyszukiwanie i zamianę danych
   e. Wykonywanie analiz danych przy użyciu formatowania warunkowego
   f. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   g. Formatowanie czasu, daty i wartości finansowych z polskim formatem
   h. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   i. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
   j. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
6. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   a. Przygotowywanie prezentacji multimedialnych, które będą:
   b. Prezentowanie przy użyciu projektora multimedialnego
   c. Drukowanie w formacie umożliwiającym robienie notatek
   d. Zapisanie jako prezentacja tylko do odczytu.
   e. Nagrywanie narracji i dołączanie jej do prezentacji
   f. Opatrywanie slajdów notatkami dla prezentera
   g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
   h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
   i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
   j. Możliwość tworzenia animacji obiektów i całych slajdów
   k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
   l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.

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

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

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

1. Wymianę informacji z możliwością wyboru i zmiany dostępnego kanału komunikacji, tj. wiadomości tekstowych (chat), rozmowy (przekazywanie dźwięku), wideo rozmowy (przekazywanie dźwięku i obrazu), współdzielenie lokalnych pulpitów w systemach Windows oraz współdzielenie dokumentów z możliwością przejmowania kontroli i edycji przez uprawnionych uczestników.
2. Kontakt poprzez wymienione kanały w modelu jeden do jednego, jeden do wielu, telekonferencji (kontakt interakcyjny wielu osób) oraz udostępniania dźwięku i obrazu dla wielu osób w sieci intranet lub internet.

3. Możliwość oceny jakości komunikacji głosowej i wideo.
4. Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze katalogowej oraz definiowania opisów użytkowników zewnętrznych w tym użytkowników wybranych bezpłatnych komunikatorów i użytkowników sieci telefonii przewodowej i komórkowej.
5. Dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką SKW lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub specjalizowanych urządzeń stacjonarnych typu telefon IP, kamera dookólna, czy duże monitory lub projektory.
6. Dostępny kliencki sprzęt peryferyjny różnych producentów posiadający potwierdzenie zgodności z SKW przez producenta SKW.
7. Dostępność informacji o statusie dostępności użytkowników na liście adresowej (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności, w tym składowanych w usłudze katalogowej.
8. Możliwość grupowania kontaktów w komunikacji tekstowej z możliwością konwersacji typu jeden-do-jednego, jeden-do-wielu i możliwością rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat.
9. Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.
10. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.
11. Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
12. Możliwość nagrywania telekonferencji przez uczestników.
13. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
14. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
15. Wbudowane funkcjonalności: SIP Proxy.
16. Wbudowana funkcjonalność mostka konferencyjnego MCU.
17. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
18. Kodowanie video H.264,
19. Wsparcie dla adresacji IPv4 i IPv6,
20. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
21. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników,
22. Możliwość szyfrowania połączeń.
23. Dostępność uczestniczenia w telekonferencjach poprzez przeglądarkę dla użytkowników z poza organizacji, zaproszonych do udziału w telekonferencji z funkcjami:
    a. Dołączania do telekonferencji,
    b. Szczegółowej listy uczestników
    c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
    d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
    e. Dostępu do udostępnianych plików,
    f. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji,
24. Dostępność aplikacji klienckiej usługi SKW (komunikatora) z funkcjonalnością:
    a. Listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielania grup kontaktów typu ulubione lub ostatnie.
    b. Historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
    c. Wsparcia telekonferencji:
    a. Dołączania do telekonferencji,
    b. Szczegółowej listy uczestników,
    c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,
    d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
    e. Głosowania,
    f. Udostępniania plików i pulpitów,

g. Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,

26. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
27. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

Wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji SKW z wybranymi systemami poczty elektronicznej i portali intranet/internet oraz usługą katalogową Active Directory.

Wynikiem takiej integracji mają być następujące funkcje i cechy systemu opartego o SKW dostępne dla użytkowników posiadających odpowiednie uprawnienia licencyjne i nadane przez administratorów:

1. Wykorzystanie domenowego mechanizmu uwierzytelnienia w oparciu o usługę katalogową, jej profile użytkowników i ich grup oraz realizację fizyczną pojedynczego logowania (single sign-on) dla uprawnionego dostępu do usług SKW.
2. Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).
3. Współdziałanie mechanizmów SKW z pocztą głosowa, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:
    a. Uruchamiania funkcji komunikacyjnych SKW z wybranych interfejsów klienta poczty elektronicznej, składników pakietu biurowego czy portalu,
    b. Dostępności w tych interfejsach danych o statusie obecności innych użytkowników (np. w nagłówkach poczty elektronicznej, czy listach użytkowników portalu.
    c. Możliwość planowania rozmów czy telekonferencji bezpośrednio poprzez zaproszenia w kalendarzu klienta poczty elektronicznej, generujące link do spotkania on-line.

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

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

Usługi bezpieczeństwa wbudowane w Produkt muszą pozwalać na:

1. Zarządzanie prawami dostępu do dokumentów i poczty elektronicznej tworzonych w Usłudze poprzez ich szyfrowanie i nadawanie praw odczytu, edycji, wydruku dla konkretnych użytkowników Usługi lub grup użytkowników Usługi.
2. Wykrywanie słów kluczowych w przesyłanych wiadomościach i sygnalizowanie potencjalnego wycieku informacji.
3. Możliwość ograniczania przedziału czasowego uprawnionego dostępu użytkowników do informacji.
4. Możliwość stosowania wymogu wieloskładnikowego uwierzytelniania.

Usługi analizy danych wbudowane w Produkt muszą umożliwiać:

1. Konfigurowanie on-line kokpitów informacyjnych wizualizujących wyniki analiz danych.
2. Gotowe mechanizmy podłączania różnego rodzaju danych strukturalnych, semi-strukturalnych i niestrukturalnych.
3. Korzystanie z gotowych algorytmów i modeli analizy oraz budowa własnych modeli w języku R.

Subskrypcja pakietu biurowego

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

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

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit,
2. Wymagania odnośnie interfejsu użytkownika:
    a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu

systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
4. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
5. 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,
6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
8. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
10. 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.
11. 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 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
    p. Zapis i edycję plików w formacie PDF.

q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco,
s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.

12. 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 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
    q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

13. 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 2010, 2013 i 2016.

14. 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.

15. 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.
16. 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.
17. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
    a. Pełna polska wersja językowa interfejsu użytkownika.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Dostępność aplikacji na platformie Windows 7 lub wyższych oraz OSX 10 lub wyższych,
    d. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

e. Możliwość obsługi tekstowych wiadomości błyskawicznych w modelu jeden do jeden i jeden do wielu.
f. Możliwość komunikacji głosowej i video w modelu jeden do jeden i jeden do wielu.
g. Obsługa telekonferencji SKW:
    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 specjalizowanych urządzeń peryferyjnych zgodnych z SKW.
o. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
p. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
q. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Microsoft Exchange Online Archiving lub równoważna **Subskrypcja pakietu usług archiwizacji poczty elektronicznej -subskrypcja na użytkownika**

Subskrypcja pozwalająca archiwizować maile, załączniki i informacje bezpiecznie i zgodnie z przepisami prawa musi spełniać następujące wymagania:

A. Wymagania ogólne
1) Umożliwiać współpracę z posiadanym Środowiskiem Microsoft Office 365 Zamawiającego
2) Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy,
3) Zagwarantowanie poziomu dostępności usługi na poziomie 99,9% (lub wyższym),
4) Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm, w tym zgodności z normami ISO 27017 i 27018,
5) Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,

6) Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych,
7) Możliwość zastrzeżenia miejsca przetwarzania/składowania danych (w przypadku zaistnienia takiego scenariusza) w usłudze do terytorium krajów Unii Europejskiej.
8) Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
9) Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.
10) Zapewnić pomoc techniczną na poziomie informatycznym 24 godziny na dobę przez siedem dni w tygodni
11) Gwarancja braku dostępu do danych Zamawiającego na platformie dostawcy usługi, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.

B. Wymagania funkcjonalne
1) Usługa archiwizacji informacji musi spełniać następujące wymagania:
2) Spójny dostęp do archiwizowanych informacji z dowolnego miejsca (wiadomości poczty elektronicznej i załączniki, kalendarze),
3) Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office 365 E1, Exchange Server 2016, 2013 i 2010, Exchange Server Online
4) Ma być dostępna jako usługa dodatkowa dla skrzynek pocztowych hostowanych online.,
5) Zapewnić wszystkim subskrybentom min. 50 GB miejsca w archiwalnej skrzynce pocztowej ,
6) Ma zapewnić możliwość zbierania elektronicznych materiałów dowodowych (w tym odzyskiwania usuniętych wiadomości poczty elektronicznej z załącznikami).
7) Zapewnić administratorom możliwość zarządzania archiwami opartymi na chmurze z poziomu centrum administracyjnego programu Exchange,
8) Możliwość dostępu przez użytkowników do zarchiwizowanych wiadomości e-mail z programu Outlook i aplikacji Outlook Web Application (OWA).

Microsoft Exchange Online Plan 1 lub równoważna **Subskrypcja pakietu usługi poczty elektronicznej typ I -subskrypcja na użytkownika**

Subskrypcja powszechnie dostępnej, standardowej usługi hostowanej (on-line) typu COTS (Commercial Of-The-Shelf) ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line poczty elektronicznej.

Wymagania dotyczące usługi hostowanej:

1. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę.
2. Wbudowana usługa musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
3. 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.
4. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
5. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
6. Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych w Usłudze własnością Zamawiającego.
7. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.

8. 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.
9. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
10. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.

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:
- Posiadanego oprogramowania Outlook (2010, 2013 i 2016),
- Przeglądarki (Web Access),
- Urządzeń mobilnych.

Wymagane cechy usługi to:
- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 50 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa najnowszych funkcji Outlook 2013 i 2016, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla 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:

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 i SMS-ów.
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.

- 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 Internet Explorer, Apple Safari i Mozilla Firefox.

Microsoft Exchange Online Plan 2 lub równoważna **Subskrypcja pakietu usługi poczty elektronicznej typ II - subskrypcja na użytkownika**

Subskrypcja powszechnie dostępnej, standardowej usługi hostowanej (on-line) typu COTS (Commercial Of-The-Shelf) ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line poczty elektronicznej.
Wymagania dotyczące usługi hostowanej:

1. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę.
2. Wbudowana usługa musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
3. 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.
4. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
5. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
6. Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych w Usłudze własnością Zamawiającego.
7. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
8. 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.
9. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
10. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.

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.
e. możliwość wykorzystania przez użytkowników zaawansowanych narzędzi archiwizacyjnych, ochrony informacji oraz narzędzi poczty głosowej.

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

a. Zarządzania użytkownikami poczty,
b. Wsparcia migracji z innych systemów poczty,
c. Wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
d. Wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty.

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

- Posiadanego oprogramowania Outlook (2010, 2013 i 2016),
- Przeglądarki (Web Access),
- Urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 30 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa najnowszych funkcji Outlook 2013 i 2016, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla 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:

11. 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.

12. 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 i SMS-ów.
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.

13. 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.

14. Wsparcie dla użytkowników mobilnych:

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

Możliwość „lekkiej” synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone
Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej
Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

Microsoft Project Online Essentials lub równoważna **Subskrypcja pakietu zarządzania projektami typ I - subskrypcja na użytkownika**

Subskrypcja usługi zarządzania projektami pozwalająca na:
1. Możliwość wyboru jeżyka interfejsu użytkownika, w tym języka polskiego i angielskiego.
2. Dostępność usługi na poziomie 99,9%.
3. Certyfikacja usługi dla normy ISO 27001.
4. Obecność tzw. klauzul umownych Unii Europejskiej (EU Model Clauses) w umowie na wykorzystanie usługi.
5. Zagwarantowane w usłudze mechanizmy składowania danych (backup) i ich odtwarzania.
6. Zarządzanie zadaniami projektowymi poprzez interfejs przeglądarki internetowej,
7. Współdzielenie dokumentów projektowych,
8. Dostępność informacji o dostępności uczestników projektu wykorzystujących usługę,
9. Synchronizację zadań projektowych z portalem wielofunkcyjnym,
10. Dystrybucję kart czasu pracy
11. Kompatybilność z Subskrypcją pakietu zarządzania projektami typ II i typ III.

Microsoft Project Online Professional lub równoważna **Subskrypcja pakietu zarządzania projektami typ II - subskrypcja na użytkownika**

Subskrypcja usługi zarządzania projektami pozwalająca na:
1. Możliwość wyboru języka interfejsu użytkownika, w tym języka polskiego i angielskiego.
2. Dostępność usługi na poziomie 99,9%.
3. Certyfikacja usługi dla normy ISO 27001.
4. Obecność tzw. klauzul umownych Unii Europejskiej (EU Model Clauses) w umowie na wykorzystanie usługi.
5. Zagwarantowane w usłudze mechanizmy składowania danych (backup) i ich odtwarzania.
6. Zarządzanie zadaniami projektowymi,
7. Współdzielenie dokumentów projektowych,
8. Synchronizację zadań projektowych z portalem wielofunkcyjnym,
9. Dystrybucję kart czasu pracy.
10. Zarządzania projektami.
11. Wykorzystanie środowiska portalu wielofunkcyjnego jako interfejsu użytkownika.
12. Współdziałanie z kalendarzami systemu Exchange w zakresie przepływu informacji o zadaniach i ich aktualizacji, z wyłączeniem informacji typu out-of-office (poza biurem).
13. Wykorzystanie otwartego standardu OData do wyszukiwania danych i ich analizy.
14. 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.
15. Możliwość wykorzystania profili użytkowników lub ich grup z usługi katalogowej przy udzielaniu uprawnień dostępu.
16. Kontrola, rozpatrywanie i zatwierdzanie dokumentów za pomocą definiowalnego przepływu pracy (workflow),
17. Możliwość definiowania przepływu pracy przy pomocy oprogramowania Visio.
18. 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 odpowiedzialności za realizację poszczególnych zadań i projektów,

19. Dostęp do funkcji systemu poprzez przeglądarkę Internet Explorer (wersja 8 lub wyższa), Firefox, Safari i Chrome.
20. 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,

2. Zarządzanie portfelami projektów

Usługa musi zapewniać dostępność instalacji pakietu zarządzania projektami, zapewniającego możliwość wspomagania dla prowadzenia projektów, między innymi w zakresie tworzenia, oraz wdrażania szablonów planów projektów. Ma zapewnić rozwiązania umożliwiające elastyczne zarządzanie pracą oraz narzędzia do współpracy potrzebne kierownikom projektów. Wraz z rozwojem potrzeb ma umożliwić korzystanie z bardziej zaawansowanych narzędzi do zespołowego zarządzania projektami. Zarządzanie projektami ma zapewnić uzyskanie jednolitych raportów

przedstawianych przełożonym oraz instytucjom zewnętrznym, w tym jednostkom prowadzącym audyty projektów.
Pakiet musi umożliwiać planowanie i udostępnianie wymaganych informacji o projekcie, takich jak:
1. Definiowanie projektów,
2. Przygotowanie harmonogramów,
    a. Opis listy zadań do wykonania
    b. Określenie struktury hierarchicznej zadań (WBS)
    c. Określenie zależności między zadaniami – relacje,
3. Tworzenie planów bazowych
4. Zapisywanie projektów,
5. Przygotowanie szablonów harmonogramów i opublikowanie ich do repozytorium szablonów,
6. Automatyczne przekształcanie inicjatyw projektowych w projekty przy wykorzystaniu szablonów projektowych,
7. W zależności od wybranych kategorii dla inicjatywy projektowej, tworzony projekt powinien zawierać harmonogram charakterystyczny dla danego typu projektu,
8. Opcje automatycznego planowania terminów zadań, wyliczające daty i okresy trwania.
9. Wizualizacja osi czasu przedstawiającej harmonogram i plan projektu.
10. Wsparcie dla planowania kroczącego i tworzenia prognoz, wykorzystujących ręcznie wprowadzone do harmonogramu zadania sumaryczne Top Down.
11. Identyfikacja braków zasobów poprzez porównanie zaplanowanych ręcznie zadań sumarycznych z informacjami spływającymi z podzadań.
12. Definicja aktywnych i nieaktywnych zadań, umożliwiająca przeprowadzenie analizy wielowariantowej.
13. Bilansowanie nadmiernie przydzielonych zasobów – zarówno automatycznie dla całego harmonogramu, jak i ręcznie dla poszczególnych zadań.
14. Grupowanie projektów według zadanych kryteriów,
    a. Etap projektu,
    b. Lokalizacja projektu,
    c. Kierownik projektu,
    d. Itp.
15. Sygnalizacja graficzna opóźnienia zadania względem planu bazowego
    a. Informacja czy jest plan bazowy,
    b. Informacja o odchyleniu względem czasu,
    c. Informacja o odchylenia względem kosztu,
    d. Informacja o odchyleniach względem pracy,
16. Śledzenie postępu realizacji projektu
    a. Analiza czasu,
    b. Analiza kosztu,
    c. Analiza godzin przepracowanych,
17. Zmiana właściciela projektu,
18. Dynamiczna zmiana właściciela projektu, zgodnie z wyborem kierownika projektu,
19. Kontrola zmian pól opisujących projekt – zmianę pól może dokonywać tylko administrator lub biuro projektów.
20. Łatwą analizę danych poprzez definiowanie filtrów dla kolumn.
21. Szeroki zakres formatowania tekstu.
22. Natywna integracja z składnikami pakietu biurowego między innymi poprzez możliwość przenoszenia informacji do aplikacji pakietu biurowego przy zachowaniu formatowania dzięki funkcjom kopiowania i wklejania.
23. Integracja ze środowiskiem serwera zarządzania projektami – pełna, dwukierunkowa synchronizacja danych.
24. Możliwość przypisywania zasobów z Active Directory.
25. Kompatybilność z Subskrypcją pakietu zarządzania projektami typ I i typ III.

Microsoft Project Online Premium lub równoważna **Subskrypcja pakietu zarządzania projektami typ III -subskrypcja na użytkownika**

Subskrypcja usługi zarządzania projektami pozwalająca na:
1. Możliwość wyboru języka interfejsu użytkownika, w tym języka polskiego i angielskiego.
2. Dostępność usługi na poziomie 99,9%.

3. Certyfikacja usługi dla normy ISO 27001.
4. Obecność tzw. klauzul umownych Unii Europejskiej (EU Model Clauses) w umowie na wykorzystanie usługi.
5. Zagwarantowane w usłudze mechanizmy składowania danych (backup) i ich odtwarzania.
6. Zarządzanie zadaniami projektowymi,
7. Współdzielenie dokumentów projektowych,
8. Synchronizację zadań projektowych z portalem wielofunkcyjnym,
9. Dystrybucję kart czasu pracy.
10. Zarządzania projektami i portfelami projektów.
11. Wykorzystanie środowiska portalu wielofunkcyjnego, jako interfejsu użytkownika.
12. 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.
13. Współdziałanie z kalendarzami systemu Exchange w zakresie przepływu informacji o zadaniach i ich aktualizacji, z wyłączeniem informacji typu out-of-office (poza biurem).
14. Wykorzystanie otwartego standardu OData do wyszukiwania danych i ich analizy.
15. 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.
16. Możliwość wykorzystania profili użytkowników lub ich grup z usługi katalogowej przy udzielaniu uprawnień dostępu.
17. Kontrola, rozpatrywanie i zatwierdzanie dokumentów za pomocą definiowalnego przepływu pracy (workflow),
18. Możliwość definiowania przepływu pracy przy pomocy oprogramowania Visio.
19. 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.
20. Dostęp do funkcji systemu poprzez przeglądarkę Internet Explorer (wersja 8 lub wyższa), Firefox, Safari i Chrome.
21. 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,

2. Zarządzanie portfelami projektów

System zarządzania projektami ma zapewnić sprawną koordynację i zarządzanie wszystkimi prowadzonymi projektami poprzez ustalenie zależności między projektami i używanymi do nich zasobami. W związku z tym system musi posiadać następujące cechy:

a. Narzędzia pozwalające na wybór optymalnego portfela projektów dostosowany do różnych ograniczeń, w tym budżetowych.
b. Analizy pozwalające określić priorytetowe projekty ze względu na wiele czynników – wartość strategiczną, wartość finansową i ryzyko.
c. Narzędzia pozwalające porównywać scenariusze optymalizacji projektów za pomocą kart wyników.
d. Narzędzia pozwalające na zmianę terminów projektów wewnątrz horyzontu czasowego planowania, w celu zoptymalizowania wykorzystania zasobów przy zachowaniu współzależności projektów.

Usługa musi zapewniać dostępność instalacji pakietu zarządzania projektami, zapewniającego możliwość wspomagania dla prowadzenia projektów, między innymi w zakresie tworzenia, oraz wdrażania szablonów planów projektów. Ma zapewnić rozwiązania umożliwiające elastyczne zarządzanie pracą oraz narzędzia do współpracy potrzebne kierownikom projektów. Wraz z rozwojem potrzeb ma umożliwić korzystanie z bardziej zaawansowanych narzędzi do zespołowego zarządzania projektami i portfelem projektów. Zarządzanie projektami ma zapewnić uzyskanie jednolitych raportów przedstawianych przełożonym oraz instytucjom zewnętrznym, w tym jednostkom prowadzącym audyty projektów.

Pakiet musi umożliwiać planowanie i udostępnianie wymaganych informacji o projekcie, takich jak:

1. Definiowanie projektów,
2. Przygotowanie harmonogramów,
   a. Opis listy zadań do wykonania
   b. Określenie struktury hierarchicznej zadań (WBS)
   c. Określenie zależności między zadaniami – relacje,
3. Tworzenie planów bazowych
4. Zapisywanie projektów,
5. Przygotowanie szablonów harmonogramów i opublikowanie ich do repozytorium szablonów,
6. Automatyczne przekształcanie inicjatyw projektowych w projekty przy wykorzystaniu szablonów projektowych,
7. W zależności od wybranych kategorii dla inicjatywy projektowej, tworzony projekt powinien zawierać harmonogram charakterystyczny dla danego typu projektu,
8. Opcje automatycznego planowania terminów zadań, wyliczające daty i okresy trwania.
9. Wizualizacja osi czasu przedstawiającej harmonogram i plan projektu.
10. Wsparcie dla planowania kroczącego i tworzenia prognoz, wykorzystujących ręcznie wprowadzone do harmonogramu zadania sumaryczne Top Down.

11. Identyfikacja braków zasobów poprzez porównanie zaplanowanych ręcznie zadań sumarycznych z informacjami spływającymi z podzadań.
12. Definicja aktywnych i nieaktywnych zadań, umożliwiająca przeprowadzenie analizy wielowariantowej.
13. Bilansowanie nadmiernie przydzielonych zasobów – zarówno automatycznie dla całego harmonogramu, jak i ręcznie dla poszczególnych zadań, także w obszarze portfela projektów.
14. Grupowanie projektów według zadanych kryteriów,
    a. Etap projektu,
    b. Lokalizacja projektu,
    c. Kierownik projektu,
    d. Itp.
15. Sygnalizacja graficzna opóźnienia zadania względem planu bazowego
    a. Informacja czy jest plan bazowy,
    b. Informacja o odchyleniu względem czasu,
    c. Informacja o odchylenia względem kosztu,
    d. Informacja o odchyleniach względem pracy,
16. Śledzenie postępu realizacji projektu
    a. Analiza czasu,
    b. Analiza kosztu,
    c. Analiza godzin przepracowanych,
17. Zmiana właściciela projektu,
18. Dynamiczna zmiana właściciela projektu, zgodnie z wyborem kierownika projektu,
19. Kontrola zmian pól opisujących projekt – zmianę pól może dokonywać tylko administrator lub biuro projektów.
20. Łatwą analizę danych poprzez definiowanie filtrów dla kolumn.
21. Szeroki zakres formatowania tekstu.
22. Natywna integracja z składnikami pakietu biurowego między innymi poprzez możliwość przenoszenia informacji do aplikacji pakietu biurowego przy zachowaniu formatowania dzięki funkcjom kopiowania i wklejania.
23. Integracja ze środowiskiem serwera zarządzania projektami – pełna, dwukierunkowa synchronizacja danych.
24. Możliwość przypisywania zasobów z Active Directory.
25. Kompatybilność z Subskrypcją pakietu zarządzania projektami typ I i typ II.

Microsoft Visio Online P1 lub równoważna **Subskrypcja pakietu modelowania graficznego typ I - subskrypcja na użytkownika**

Pakiet usług graficznego modelowania w postaci wektorowej: procesów biznesowych, procesów obiegu informacji, schematów organizacyjnych, diagramów sieciowych, harmonogramów.
Pakiet musi zapewniać:

1. Możliwość otwierania i przeglądania rysunków przy użyciu bezpłatnie dostępnego narzędzia.
2. Pracę online za pomocą przeglądarki internetowej.
3. Zgodność z interfejsem dotykowym Windows.
4. Zapis danych w postaci plików XML.
5. Możliwość importu i eksportu do formatu plików zgodnych z AutoCad.
6. Możliwość graficznego obrazowania i analizowania danych pobieranych z plików xls i xlsx, baz danych dostępnych przez ODBC na diagramach.
7. Udostępnianie kreatorów budowy diagramów.
8. Udostępnianie gotowych kształtów (shape) opisanych metadanymi i możliwość kreowania i edycji kształtów.
9. Możliwość zmiany kształtu przy zachowaniu jego metadanych oraz całości diagramu.
10. Możliwość budowy diagramów przestawnych, które są kolekcją kształtów uporządkowanych w strukturę drzewa, która pomaga analizować dane i podsumowywać je w zrozumiałym formacie wizualnym. Taki diagram zaczyna się od kształtu nazywanego węzłem najwyższego poziomu, który zawiera informacje zaimportowane z arkusza, tabeli, widoku lub modułu. Węzeł najwyższego poziomu można podzielić na poziom węzłów podrzędnych, aby dane można było wyświetlać w różny sposób.
11. Udostępnianie gotowych szablonów służących do wizualizowania i usprawniania procesów biznesowych, śledzenia projektów i zasobów, układania schematów organizacji, mapowania

sieci, tworzenia diagramów obszarów budowy i optymalizacji systemów. Wymagane są szablony graficznego modelowania w postaci wektorowej:
   a. procesów biznesowych,
   b. procesów obiegu informacji,
   c. schematów organizacyjnych,
   d. diagramów sieciowych,
   e. harmonogramów.
12. Funkcja autołączenia, która automatycznie łączy kształty, równomiernie je rozmieszcza i wyrównuje do założonej siatki. Przenoszenie połączonych kształtów nie rozłącza ich, tylko powoduje automatyczne wytyczenie nowej trasy łącznika między nimi.
13. Połączenie diagramów z danymi umożliwiające uzyskanie obrazu procesu, projektu lub systemu pozwalające na identyfikowanie kluczowych trendów, problemów i wyjątków, a następnie określanie właściwego sposobu postępowania.
14. Graficzne raporty z informacjami o projektach do wizualizacji kompleksowych informacji o projektach.

Microsoft Visio Online Plan 2 lub równoważna **Subskrypcja pakietu modelowania graficznego typ II - subskrypcja na użytkownika**

Pakiet usług do graficznego modelowania w postaci wektorowej: procesów biznesowych, procesów obiegu informacji, schematów organizacyjnych, diagramów sieciowych, harmonogramów wraz możliwością instalacji pakietu na komputerze klasy PC.
Pakiet musi zapewniać:
1. Możliwość otwierania i przeglądania rysunków przy użyciu bezpłatnie dostępnego narzędzia.
2. Zgodność z interfejsem dotykowym Windows.
3. Możliwość pracy kilku osób na jednym diagramie w tym samym czasie.
4. Zapis danych w postaci plików XML.
5. Zgodność ze standardami:
   a. Unified Modeling Language (UML) 2.4,
   b. Business Process Model and Notation (BPMN) 2.0.
6. Publikacja przepływów pracy dla SharePoint.
7. Możliwość importu i eksportu do formatu plików zgodnych z AutoCad.
8. Możliwość graficznego obrazowania i analizowania danych pobieranych z plików xls i xlsx, baz danych dostępnych przez ODBC na diagramach.
9. Udostępnianie kreatorów budowy diagramów.
10. Udostępnianie gotowych kształtów (shape) opisanych metadanymi i możliwość kreowania i edycji kształtów.
11. Możliwość zmiany kształtu przy zachowaniu jego metadanych oraz całości diagramu.
12. Możliwość budowy diagramów przestawnych, które są kolekcją kształtów uporządkowanych w strukturę drzewa, która pomaga analizować dane i podsumowywać je w zrozumiałym formacie wizualnym. Taki diagram zaczyna się od kształtu nazywanego węzłem najwyższego poziomu, który zawiera informacje zaimportowane z arkusza, tabeli, widoku lub modułu. Węzeł najwyższego poziomu można podzielić na poziom węzłów podrzędnych, aby dane można było wyświetlać w różny sposób.
13. Udostępnianie gotowych szablonów służących do wizualizowania i usprawniania procesów biznesowych, śledzenia projektów i zasobów, układania schematów organizacji, mapowania sieci, tworzenia diagramów obszarów budowy i optymalizacji systemów. Wymagane są szablony graficznego modelowania w postaci wektorowej:
   a. procesów biznesowych,
   b. procesów obiegu informacji,
   c. schematów organizacyjnych,
   d. diagramów sieciowych,
   e. harmonogramów.
14. Funkcja autołączenia, która automatycznie łączy kształty, równomiernie je rozmieszcza i wyrównuje do założonej siatki. Przenoszenie połączonych kształtów nie rozłącza ich, tylko powoduje automatyczne wytyczenie nowej trasy łącznika między nimi.
15. Połączenie diagramów z danymi umożliwiające uzyskanie obrazu procesu, projektu lub systemu pozwalające na identyfikowanie kluczowych trendów, problemów i wyjątków, a następnie określanie właściwego sposobu postępowania.

16. Graficzne raporty z informacjami o projektach do wizualizacji kompleksowych informacji o projektach. Umożliwienie generowania raportów, które pozwalają śledzić informacje o zadaniach, właścicielach, rolach i obowiązkach dotyczących projektów, a także przedstawiają złożone struktury własności w projekcie.
17. Możliwość automatycznego modyfikowania raportów w miarę zmian informacji o projektach.

Azure Information Protection Premium P1 lub równoważna **Subskrypcja pakietu usług hostowanych ochrony informacji typ I - subskrypcja na użytkownika**

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

1. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,
2. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
3. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
4. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
5. Możliwość 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.

Azure Information Protection Premium P2 lub równoważna **Subskrypcja pakietu usług hostowanych ochrony informacji typ II - subskrypcja na użytkownika**

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

1. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,

2. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
3. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
4. Możliwość klasyfikacji informacji wraz z możliwością narzucania użytkownikom automatycznej klasyfikacji danych.
5. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
6. Możliwość szyfrowania informacji przy użyciu własnych kluczy.
7. 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.
8. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
9. Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji,
10. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej" instalacji w całej organizacji,
11. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
12. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.
13. Scentralizowane zarządzanie przydzielania dostępu do aplikacji,
14. Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),
15. Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),
16. Samoobsługowe resetowania hasła.
17. Dostarczanie mechanizmów usługi uwierzytelniania użytkowników,
18. Konsolę zarządzania tożsamością i dostępem.

Office 365 Advanced Treat Protection lub równoważna **Subskrypcja pakietu usług hostowanych bezpieczeństwa informacji - subskrypcja na użytkownika**

Subskrypcja pakietu usług hostowanych bezpieczeństwa informacji musi pozwalać na ochronę informacji w wiadomościach poczty elektronicznej, plikach i aplikacjach pakietu biurowego.
Pakiet musi zapewniać:

1. Ochronę skrzynek poczty elektronicznej przed zaawansowanymi atakami.
2. Ochronę przed atakami typu zero-day.
3. Behawioralną analizę załączników wiadomości w wykorzystaniem technik uczenia maszynowego.
4. Poddawanie wiadomości zawierających podejrzane linki lub załączniki kwarantannie.
5. Mechanizm detonacji podejrzanych załączników w środowisku maszyn wirtualnych przed dostarczeniem użytkownikowi.
6. Ochronę przed linkami do niebezpiecznych treści lub oprogramowania poprzez skanowanie źródeł tych łączy, przepisanie adresów linków, z zakwalifikowaniem jako bezpieczne lub wyświetlaniu informacji o zablokowaniu niebezpiecznych stron.
7. Dostarczanie informacji uprawnionym administratorom o uruchamianiu przez użytkownika linków zakwalifikowanych jako niebezpieczne.
8. Dostarczanie informacji uprawnionym administratorom o tym którzy użytkownicy byli celami poszczególnych ataków.
9. Wykrywanie nietypowych przypadków wysyłania wiadomości w imieniu innego użytkownika.
10. Techniki uczenia maszynowego dla wykrywania nieznanych wzorów ataku.

Office 365 Data Loss Prevention lub równoważna **Subskrypcja pakietu usług hostowanych przeciwdziałania wyciekom informacji - subskrypcja na użytkownika**

Subskrypcja pakietu usług hostowanych bezpieczeństwa informacji musi pozwalać na ochronę informacji w wiadomościach poczty elektronicznej, plikach i aplikacjach pakietu biurowego typu Data Loss Prevention (DLP),

1. Usługa musi bazować na zestawie uprzednio skonstruowanych reguł przeszukiwania wrażliwych informacji.
2. Działanie systemu DLP musi zakładać przeszukiwanie e-maili pod kątem słów kluczowych zawartych w temacie, treści wiadomości i załączonych dokumentach.
3. Przy użyciu predefiniowanego słownika usługa ma wykrywać wiadomości, które zawierają poufne i wrażliwe dane, oraz wszystkie inne informacje istotne z perspektywy funkcjonowania Zamawiającego, w tym dane osobowe.
4. Warunki śledzenia korespondencji definiowane mają być przez administratorów.
5. System DLP ma umożliwić sterowanie przepływem poczty sklasyfikowanej jako zawierającej wrażliwe dane. Każda taka wiadomość może zostać zablokowana przed wysłaniem lub przekazana do moderacji.
6. System ma informować administratora bezpieczeństwa o zaistniałym incydencie.

Microsoft Enterprise Mobility + Security lub równoważna **Subskrypcja pakietu usług zarządzania urządzeniami oraz tożsamością użytkowników - subskrypcja na użytkownika**

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

Wymagania ogólne

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

18. Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.
19. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.

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

Wymagane scenariusze użycia:
1. Możliwość wykorzystania telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS lub specjalizowanych aplikacji, potwierdzających tożsamość użytkownika podczas dostępu do aplikacji webowych pozwalające na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia, lub z poza sieci lokalnej.
2. Możliwość pracy na prywatnych urządzeniach użytkowników zapewniający bezpieczny i kontrolowany dostęp do danych i aplikacji, w możliwością wydzielenia i usunięcia danych służbowych z urządzenia,
3. Jednokrotne logowanie (single sign-on)w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika, przy zachowaniu niezaprzeczalności działań,
4. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwalający na redukcję ilości zgłoszeń działów wsparcia,
5. Automatyczne przepływy pracy i reguł biznesowych pozwalające przyspieszenie procesów i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie ustalonych polityk i procedur),
6. Zarządzanie urządzeniami mobilnymi pozwalające na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwiające zdalne kasowanie danych firmowych lub całego urządzenia.

Podsystem zarządzania tożsamością:
System zarządzania tożsamością elektroniczną ma zapewniać pobieranie, agregację oraz synchronizacje danych o użytkownikach z różnych systemów w ramach organizacji wraz z zarządzaniem certyfikatami wydawanymi w ramach własnego centrum certyfikacji (CA).
Bezpieczeństwo
1. System zarządzania tożsamością musi umożliwiać zastosowanie - przy połączeniu ze źródłami danych - mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji).
2. System musi zapewniać prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej zaporami *firewall* oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
3. System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
4. System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.

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

Interoperacyjność
6. System zarządzania tożsamością musi zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem.

7. System zarządzania tożsamością musi zapewniać możliwość realizacji dwukierunkowej, uprawnionej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.

Skalowalność funkcjonalna

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

Wydajność

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

Wymagania w zakresie cech i funkcjonalności rozwiązania

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

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

    c. System musi zapewniać możliwość komunikacji z powyższymi informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
    d. System musi zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy integrujące poprzez budowę odpowiedniego rozszerzenia systemu.
    e. System musi zapewniać możliwość uprawnionego tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.
    f. System musi dostarczać mechanizmy pozwalające na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
    g. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system musi umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium, umożliwiając synchronizację danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
    h. System musi oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
    i. System musi umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.
2. Repozytorium danych teleadresowych
    a. System musi umożliwiać agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.
    b. System misi zapewnić interfejs użytkownika zapewniający możliwość wyszukiwania oraz przeglądania danych dla wszystkich uprawnionych użytkowników systemu.
    c. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie dostępu, zarządzania oraz uaktualnienia danych teleadresowych.
    d. W ramach interfejsu użytkownika system musi zapewniać możliwość udostępnienia edycji zakresu udostępnianych danych samodzielnie przez każdego z uprawnionych użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.
3. Zarządzanie kartą elektroniczną

a. Zarządzanie kartami elektronicznymi musi obejmować: personalizację graficzną kart (nadruk), zdalne zarządzania PIN'ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów),
b. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 10 000 użytkowników,
c. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnym przechowywanym i wygenerowanym na karcie)
d. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania itp.,
e. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP,
f. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI,
g. System musi wspierać zarządzanie certyfikatami używanymi do uwierzytelnienia w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.
h. System musi umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów,
i. Po wystawieniu certyfikatu, system musi umożliwić włączenie automatycznej publikacji certyfikatu w katalogu LDAP,
j. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP,
k. Certyfikaty wystawione na jednej stacji muszą być automatycznie dostępne dla użytkownika na innej stacji o ile się tam zaloguje (dotyczy certyfikatów przechowywanych w profilu użytkownika jak i certyfikatów przechowywanych na karcie elektronicznej),
l. Systemu musi posiadać przyjazny interfejs oparty o WWW, przez który użytkownik końcowy może wykonywać operacje zarządzania swoimi certyfikatami i PIN'ami dostępowymi (zmiana PIN'u, odblokowanie karty),
m. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/ wygenerowanie PIN'u inicjującego do karty elektronicznej następującymi drogami:

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

n. Personalizacją graficzna musi pobierać ze wskazanego przez Zamawiającego źródła danych, zdjęcia pracowników i umieszczać je wraz z innymi danymi identyfikacyjnymi na karcie.
o. System musi umożliwiać odblokowanie kart w oparciu o autoryzację użytkownika w katalogu LDAP z wykorzystaniem hasła jednokrotnego,
p. Bezpośrednie odblokowanie karty musi być wykonywane w oparciu mechanizm challenge/response (zabrania stosowania się SO PIN'u statycznego),
q. Na PIN'y wykorzystywane przez użytkownika musi być możliwość nakładania polityk bezpieczeństwa definiujących stopień skomplikowania PIN'u, w szczególności:

- nie mniej niż 6 znaków,
- wymagane cyfry litery małe i duże,
- PIN może się powtarzać przez N zmian,

r. System musi wspierać karty Cryptotech MultiliSign 2.0 lub równoważne,
s. Zarządzanie wystawianiem certyfikatów musi się odbywać w oparciu o definiowalny przepływ roboczy (workflow), który będzie mógł być modyfikowany bezpośrednio przez operatora systemu z poziomu interfejsu graficznego,
t. Workflow musi umożliwiać, implementację następujących scenariuszy użycia:

- w pełni automatyczne wystawianie certyfikatów dla użytkowników,
- wystawianie certyfikatów wymagające każdorazowej aprobaty operatora systemu,

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

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

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

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

v. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, liczby zmian PIN'ow, czy liczby odblokowanych kart,
w. Dane służące do deszyfracji kluczy prywatnych użytkowników przechowywanych w systemie, muszą być bezpiecznie składowane na urządzeniu HSM typu nCipher netHSM 500 lub w pełni równoważnych,
x. Bezpośrednie zarządzanie kartami musi odbywać się przez dostarczany wraz z systemem Microsoft Windows interfejs „Microsoft Smart Card Base CSP" lub standard PKCS#11,
y. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania),

Podsystem zarządzania urządzeniami mobilnymi

1. Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:
   a. Integrację z systemem Microsoft SCCM w oparciu o natywne interfejsy komunikacyjne
   b. Wykorzystanie bazy użytkowników znajdujących się w Active Directory
   c. Inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych,
   d. Inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji:
      i. Nazwa urządzenia
      ii. Identyfikator urządzenia
      iii. Nazwa platformy systemu operacyjnego
      iv. Wersja oprogramowania układowego
      v. Typ procesora
      vi. Model urządzenia
      vii. Producent urządzenia
      viii. Architektura procesora
      ix. Język urządzenia
      x. Lista aplikacji zainstalowanych w ramach przedsiębiorstwa
2. W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).
3. Wymagania w zakresie dystrybucji oprogramowania:
   a. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
   b. Usługa ma umożliwiać dystrybucję oprogramowania na żądanie użytkownika, realizowane poprzez wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji

c. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
d. Katalog aplikacji ma wspierać następujące formaty aplikacji mobilnych:
   i. *. appx (Windows RT)
   ii. *.ipa (iOS)
   iii. *.apk (Android)
e. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:
   i. Windows Store
   ii. Windows Phone Store
   iii. Android Google Play Store
   iv. iOS App Store

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

Podsystem ochrony informacji

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

1. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,
2. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
3. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
4. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
5. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, w tym:
   a. Brak uprawnień dostępu do informacji,
   b. Informacja tylko do odczytu,
   c. Prawo do edycji informacji,
   d. Brak możliwości wykonania systemowego zrzutu ekranu,
   e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
   f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
   g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.
6. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
7. Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji,
8. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji,
9. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android i Windows RT,
10. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

Podsystem usługi uwierzytelniania

Usługa uwierzytelniania musi zapewnić:
1. Możliwość zintegrowania jednokrotnego logowania (SSO) dla popularnych aplikacji typu SaaS,
2. Gotowe mechanizmy uwierzytelniania do aplikacji webowych dla użytkowników zewnętrznych,
3. Możliwość połączenia lub synchronizacji z usługą Active Directory wewnątrz organizacji,
4. Scentralizowane zarządzanie przydzielania dostępu do aplikacji,
5. Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),
6. Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),
7. Samoobsługowe resetowania hasła,
8. Dostarczanie mechanizmów usługi katalogowej uwierzytelniania użytkowników,
9. Konsolę zarządzania tożsamością i dostępem.

Azure Multifactor Authentication lub równoważna **Subskrypcja pakietu usługi uwierzytelniania wieloskładnikowego – subskrypcja na użytkownika**

Subskrypcja pakietu dodatkowych usług do pakietów usług hostowanych opisanych w SIWZ pozwalających na wykorzystanie uwierzytelnienia wieloskładnikowego.

Microsoft 365 E3 lub równoważna **Subskrypcja pakietów usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego typ I - subskrypcja na użytkownika**

Subskrypcja pakietów usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego musi zawierać następujące oprogramowanie i usługi:

System operacyjny klasy desktop

System operacyjny klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
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, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe,
4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
5. Wbudowany system pomocy w języku polskim;
6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
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 PINu. Mechanizm musi być zgodny ze specyfikacją FIDO.
27. Mechanizmy 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 mikrochipie 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.

Subskrypcja usługi hostowanej i pakietu biurowego

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

Wymagania dotyczące usługi hostowanej:

1. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę katalogową.
2. Wbudowana usługa LDAP musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
3. Możliwość dodawania własnych nazw domenowych do usługi katalogowej.
4. Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup.
5. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
6. 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.
7. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
8. Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich.
9. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
10. Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych w Usłudze własnością Zamawiającego.

11. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
12. 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.
13. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
14. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.

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:

a. Posiadanego oprogramowania Outlook (2010, 2013 i 2016),
b. Przeglądarki (Web Access),
c. Urządzeń mobilnych.

Wymagane cechy usługi to:

a. Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 50 GB,
b. Standardowy i łatwy sposób obsługi poczty elektronicznej,
c. Obsługa najnowszych funkcji Outlook 2013 i 2016, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Firefox i Safari,
d. Współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy.
e. Bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

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

- 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.

- 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.

- 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.

- Wsparcie dla użytkowników mobilnych:

Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu opisanej w punkcie a). Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem
Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone
Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej
Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

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

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych,
2. Zarządzanie strukturą portalu i treściami www,
3. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
4. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej,
5. Tworzenie repozytoriów wzorów dokumentów,
6. Tworzenie repozytoriów dokumentów,
7. Wspólną, bezpieczną pracę nad dokumentami,
8. Wersjonowanie dokumentów (dla wersji roboczych),
9. Organizację pracy grupowej,
10. Wyszukiwanie treści,
11. Dostęp do danych w relacyjnych bazach danych,
12. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

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

1. Interfejs użytkownika:
   a. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
   b. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0
   c. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
   d. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
   e. 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 2010 i 2016z zapewnieniem konwersji wszystkich elementów i atrybutów dokumentu
   m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
5. Arkusz kalkulacyjny musi umożliwiać:
   a. Tworzenie raportów tabelarycznych
   b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
   c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d. Wyszukiwanie i zamianę danych
   e. Wykonywanie analiz danych przy użyciu formatowania warunkowego
   f. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   g. Formatowanie czasu, daty i wartości finansowych z polskim formatem
   h. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   i. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
   j. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
6. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   a. Przygotowywanie prezentacji multimedialnych, które będą:
   b. Prezentowanie przy użyciu projektora multimedialnego
   c. Drukowanie w formacie umożliwiającym robienie notatek
   d. Zapisanie jako prezentacja tylko do odczytu.
   e. Nagrywanie narracji i dołączanie jej do prezentacji
   f. Opatrywanie slajdów notatkami dla prezentera
   g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo

h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
j. Możliwość tworzenia animacji obiektów i całych slajdów
k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.

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

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

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

1. Wymianę informacji z możliwością wyboru i zmiany dostępnego kanału komunikacji, tj. wiadomości tekstowych (chat), rozmowy (przekazywanie dźwięku), wideo rozmowy (przekazywanie dźwięku i obrazu), współdzielenie lokalnych pulpitów w systemach Windows oraz współdzielenie dokumentów z możliwością przejmowania kontroli i edycji przez uprawnionych uczestników.
2. Kontakt poprzez wymienione kanały w modelu jeden do jednego, jeden do wielu, telekonferencji (kontakt interakcyjny wielu osób) oraz udostępniania dźwięku i obrazu dla wielu osób w sieci intranet lub internet.
3. Możliwość oceny jakości komunikacji głosowej i wideo.
4. Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze katalogowej oraz definiowania opisów użytkowników zewnętrznych w tym użytkowników wybranych bezpłatnych komunikatorów i użytkowników sieci telefonii przewodowej i komórkowej.
5. Dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką SKW lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub specjalizowanych urządzeń stacjonarnych typu telefon IP, kamera dookólna czy duże monitory lub projektory.
6. Dostępny kliencki sprzęt peryferyjny różnych producentów posiadający potwierdzenie zgodności z SKW przez producenta SKW.
7. Dostępność informacji o statusie dostępności użytkowników na liście adresowej (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności, w tym składowanych w usłudze katalogowej.
8. Możliwość grupowania kontaktów w komunikacji tekstowej z możliwością konwersacji typu jeden-do-jednego, jeden-do-wielu i możliwością rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat.
9. Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.
10. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.
11. Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
12. Możliwość nagrywania telekonferencji przez uczestników.
13. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
14. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
15. Wbudowane funkcjonalności: SIP Proxy.
16. Wbudowana funkcjonalność mostka konferencyjnego MCU.
17. Obsługa standardów: CSTA, TLS, SIP over TCP.
18. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
19. Kodowanie video H.264,
20. Wsparcie dla adresacji IPv4 i IPv6,
21. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
22. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników,

23. Możliwość szyfrowania połączeń.
24. Dostępność uczestniczenia w telekonferencjach poprzez przeglądarkę dla użytkowników z poza organizacji, zaproszonych do udziału w telekonferencji z funkcjami:
    a. Dołączania do telekonferencji,
    b. Szczegółowej listy uczestników
    c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
    d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
    e. Dostępu do udostępnianych plików,
    f. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji,
25. Dostępność aplikacji klienckiej usługi SKW (komunikatora) z funkcjonalnością:
    a. Listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielania grup kontaktów typu ulubione lub ostatnie.
    b. Historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
    c. Wsparcia telekonferencji:
    a. Dołączania do telekonferencji,
    b. Szczegółowej listy uczestników,
    c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,
    d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
    e. Głosowania,
    f. Udostępniania plików i pulpitów,
    g. Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,
28. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
29. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

Wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji SKW z wybranymi systemami poczty elektronicznej i portali intranet/internet oraz usługą katalogową Active Directory.

Wynikiem takiej integracji mają być następujące funkcje i cechy systemu opartego o SKW dostępne dla użytkowników posiadających odpowiednie uprawnienia licencyjne i nadane przez administratorów:

1. Wykorzystanie domenowego mechanizmu uwierzytelnienia w oparciu o usługę katalogową, jej profile użytkowników i ich grup oraz realizację fizyczną pojedynczego logowania (single sign-on) dla uprawnionego dostępu do usług SKW.
2. Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).
3. Współdziałanie mechanizmów SKW z pocztą głosowa, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:
    a. Uruchamiania funkcji komunikacyjnych SKW z wybranych interfejsów klienta poczty elektronicznej, składników pakietu biurowego czy portalu,
    b. Dostępności w tych interfejsach danych o statusie obecności innych użytkowników (np. w nagłówkach poczty elektronicznej, czy listach użytkowników portalu.
    c. Możliwość planowania rozmów czy telekonferencji bezpośrednio poprzez zaproszenia w kalendarzu klienta poczty elektronicznej, generujące link do spotkania on-line.

Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 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.

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:

18. Dostępność pakietu w wersjach 32-bit oraz 64-bit,
19. 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.
20. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
21. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
22. 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,
23. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
24. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
25. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
26. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
27. 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.
28. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c. Wstawianie oraz formatowanie tabel.
    d. Wstawianie oraz formatowanie obiektów graficznych.
    e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    g. Automatyczne tworzenie spisów treści.
    h. Formatowanie nagłówków i stopek stron.
    i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
    j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
    k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.

l. Określenie układu strony (pionowa/pozioma).
m. Wydruk dokumentów.
n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007, Microsoft Word 2010 i 2013 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.

29. 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 2007 oraz Microsoft Excel 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

30. 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 2007, MS PowerPoint 2010 i 2013.

31. 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.
32. 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.
33. 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.

34. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
    a. Pełna polska wersja językowa interfejsu użytkownika.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Dostępność aplikacji na platformie Windows 7 lub wyższych oraz OSX 10 lub wyższych,
    d. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
    e. Możliwość obsługi tekstowych wiadomości błyskawicznych w modelu jeden do jeden i jeden do wielu.
    f. Możliwość komunikacji głosowej i video w modelu jeden do jeden i jeden do wielu.
    g. Obsługa telekonferencji SKW:
        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 specjalizowanych urządzeń peryferyjnych zgodnych z SKW.
    o. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
    p. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
    q. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Subskrypcja usługi zarządzania urządzeniami oraz tożsamością użytkowników

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

Wymagania ogólne

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

b. Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym),
c. Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm, w tym zgodności z normami ISO 27017 i 27018,
d. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO.
e. Możliwość skalowania usługi z ustalonymi kosztami takiego skalowania,
f. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
g. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
h. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
i. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
j. Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione".
k. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
l. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
m. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
n. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych,
o. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Unii Europejskiej.
p. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
q. Mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.
r. Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.
s. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.

Wymagania funkcjonalne

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

Wymagane scenariusze użycia:

1. Możliwość wykorzystania telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS lub specjalizowanych aplikacji, potwierdzających tożsamość użytkownika podczas dostępu do aplikacji webowych pozwalające na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia, lub z poza sieci lokalnej.
2. Możliwość pracy na prywatnych urządzeniach użytkowników zapewniający bezpieczny i kontrolowany dostęp do danych i aplikacji, w możliwością wydzielenia i usunięcia danych służbowych z urządzenia,
3. Jednokrotne logowanie (single sign-on)w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika, przy zachowaniu niezaprzeczalności działań,
4. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwalający na redukcję ilości zgłoszeń działów wsparcia,
5. Automatyczne przepływy pracy i reguł biznesowych pozwalające przyspieszenie procesów i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby

w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie ustalonych polityk i procedur),

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

Podsystem zarządzania tożsamością:

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

Bezpieczeństwo

1. System zarządzania tożsamością musi umożliwiać zastosowanie - przy połączeniu ze źródłami danych - mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji).
2. System musi zapewniać prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej zaporami *firewall* oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
3. System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
4. System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.

Skalowalność

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

Interoperacyjność

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

Skalowalność funkcjonalna

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

Wydajność

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

Wymagania w zakresie cech i funkcjonalności rozwiązania

Agregacja i synchronizacja danych

a. System musi zapewniać możliwość odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą.
b. System zarządzania tożsamością, w ramach początkowego wdrożenia musi zapewnić możliwość integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:
   - Pliki tekstowe CSV, AVP, LDIF
   - Bazy danych MS SQL 2000 - 2016, Oracle
   - Usługi katalogowe Microsoft Active Directory, Novell eDirectory, OpenLDAP.
c. System musi zapewniać możliwość komunikacji z powyższymi informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
d. System musi zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy integrujące poprzez budowę odpowiedniego rozszerzenia systemu.
e. System musi zapewniać możliwość uprawnionego tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.

f. System musi dostarczać mechanizmy pozwalające na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
g. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system musi umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium, umożliwiając synchronizację danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
h. System musi oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
i. System musi umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.

Repozytorium danych teleadresowych

a. System musi umożliwiać agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.
b. System misi zapewnić interfejs użytkownika zapewniający możliwość wyszukiwania oraz przeglądania danych dla wszystkich uprawnionych użytkowników systemu.
c. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie dostępu, zarządzania oraz uaktualnienia danych teleadresowych.
d. W ramach interfejsu użytkownika system musi zapewniać możliwość udostępnienia edycji zakresu udostępnianych danych samodzielnie przez każdego z uprawnionych użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.

Zarządzanie kartą elektroniczną

a. Zarządzanie kartami elektronicznymi musi obejmować: personalizację graficzną kart (nadruk), zdalne zarządzania PIN'ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów),
b. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 10 000 użytkowników,
c. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnym przechowywanym i wygenerowanym na karcie)
d. System musi umożliwiać wydawanie i zarządzanie wieloma certyfikatami na jednej karcie (przewiduje się wykorzystanie 4 certyfikatów dla jednego użytkownika)
e. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania itp.,
f. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP,
g. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI,
h. System musi wspierać zarządzanie certyfikatami używanymi do uwierzytelnienia w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.
i. System musi umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów,
j. Po wystawieniu certyfikatu, system musi umożliwić włączenie automatycznej publikacji certyfikatu w katalogu LDAP,
k. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP,
l. Certyfikaty wystawione na jednej stacji muszą być automatycznie dostępne dla użytkownika na innej stacji o ile się tam zaloguje (dotyczy certyfikatów przechowywanych w profilu użytkownika jak i certyfikatów przechowywanych na karcie elektronicznej),
m. Systemu musi posiadać przyjazny interfejs oparty o WWW, przez który użytkownik końcowy może wykonywać operacje zarządzania swoimi certyfikatami i PIN'ami dostępowymi (zmiana PIN'u, odblokowanie karty),
n. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/ wygenerowanie PIN'u inicjującego do karty elektronicznej następującymi drogami:

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

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

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

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

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

- nie mniej niż 6 znaków,
- wymagane cyfry litery małe i duże,
- PIN może się powtarzać przez N zmian,

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

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

u. Workflow musi umożliwiać, implementacji następujących scenariuszy użycia:

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

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

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

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

a. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, liczby zmian PIN'ow, czy liczby odblokowanych kart,
b. Dane służące do deszyfracji kluczy prywatnych użytkowników przechowywanych w systemie, muszą być bezpiecznie składowane na urządzeniu HSM typu nCipher netHSM 500 lub w pełni równoważnych,
c. Bezpośrednie zarządzania kartami musi odbywać się przez dostarczany wraz z systemem Microsoft Windows interfejs „Microsoft Smart Card Base CSP" lub standard PKCS#11,
d. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania),

Podsystem zarządzania urządzeniami mobilnymi

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

a. Integrację z systemem Microsoft SCCM w oparciu o natywne interfejsy komunikacyjne
b. Wykorzystanie bazy użytkowników znajdujących się w Active Directory
c. Inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych,

d. Inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji:
   - Nazwa urządzenia
   - Identyfikator urządzenia
   - Nazwa platformy systemu operacyjnego
   - Wersja oprogramowania układowego
   - Typ procesora
   - Model urządzenia
   - Producent urządzenia
   - Architektura procesora
   - Język urządzenia
   - Lista aplikacji zainstalowanych w ramach przedsiębiorstwa

W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).

Wymagania w zakresie dystrybucji oprogramowania:

a. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
b. Usługa ma umożliwiać dystrybucję oprogramowania na żądanie użytkownika, realizowane poprzez wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji
c. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
d. Katalog aplikacji ma wspierać następujące formaty aplikacji mobilnych:
   - *. appx (Windows RT)
   - *.ipa (iOS)
   - *.apk (Android)

e. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:
   - Windows Store
   - Windows Phone Store
   - Android Google Play Store
   - iOS App Store

W obszarze polityki haseł usługa zapewni:

a. Zdefiniowanie wymuszenia hasła,
b. Określenie minimalnej długości hasła,
c. Określenie czasu wygasania hasła,
d. Określenie liczby pamiętanych haseł,
e. Określenie liczby prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia,
f. Określenie czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła.

Usługa ma umożliwiać skorzystanie z szeregu predefiniowane raportów dedykowanych dla klas urządzeń mobilnych. W szczególności w obszarze raportowania zainstalowanego oprogramowania jest możliwość zebrania informacji o zainstalowanym oprogramowaniu na urządzeniu firmowym lub urządzeniu użytkownika:

Podsystem ochrony informacji

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

1. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,

2. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
3. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
4. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
5. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, w tym:
    a. Brak uprawnień dostępu do informacji,
    b. Informacja tylko do odczytu,
    c. Prawo do edycji informacji,
    d. Brak możliwości wykonania systemowego zrzutu ekranu,
    e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
    f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
    g. Brak możliwości użycia opcji „Odpowiedz wszystkim" w poczcie elektronicznej.
6. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
7. Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji,
8. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej" instalacji w całej organizacji,
9. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
10. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

Podsystem usługi katalogowej

Usługa katalogowa musi zapewnić:

1. Możliwość zintegrowania jednokrotnego logowania (SSO) dla popularnych aplikacji typu SaaS,
2. Gotowe mechanizmy uwierzytelniania do aplikacji webowych dla użytkowników zewnętrznych,
3. Możliwość połączenia lub synchronizacji z usługą Active Directory wewnątrz organizacji,
4. Scentralizowane zarządzanie przydzielania dostępu do aplikacji,
5. Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),
6. Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),
7. Samoobsługowe resetowania hasła,
8. Dostarczanie mechanizmów usługi katalogowej uwierzytelniania użytkowników,
9. Konsolę zarządzania tożsamością i dostępem.

Microsoft 365 E5 lub równoważna **Subskrypcja pakietów usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego typ II - subskrypcja na użytkownika**

Subskrypcja pakietów usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego musi zawierać następujące oprogramowanie i usługi:

System operacyjny klasy desktop

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

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, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe,
4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
5. Wbudowany system pomocy w języku polskim;
6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,

7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.
8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.
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. Mechanizmy 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.
83. Ochrona przed atakami zawierająca mechanizmy analizy behawioralnej, dostęp do usługi analiz bezpieczeństwa i zagregowanej wizualizacji zagrożeń i anomalii.
84. Możliwość analizy stanu urządzeń w sieci i ich aktywności, przebiegu nietypowych procesów, wykorzystania plików czy nietypowych połączeń w sieci w okresie ostatnich 6 miesięcy.
85. Usługa pozwalająca na izolowanie w środowisku wirtualnym plików czy adresów sieciowych w celu kontroli.
86. Mechanizmy rekomendujące sposób postępowania w przypadku ataku.

Subskrypcja usługi hostowanej i pakietu biurowego

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

Wymagania dotyczące usługi hostowanej:

a. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę LDAP.
b. Wbudowana usługa LDAP musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
c. Możliwość dodawania do 500 własnych nazw domenowych do usługi LDAP.
d. Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup.
e. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
f. Ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day.
g. 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.
h. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
i. Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich.
j. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
k. Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych w Usłudze własnością Zamawiającego.
l. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
m. 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.
n. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
o. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.

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:
a. Posiadanego oprogramowania Outlook (2010, 2013 i 2016),
b. Przeglądarki (Web Access),
c. Urządzeń mobilnych.
Wymagane cechy usługi to:
a. Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 50 GB,
b. Standardowy i łatwy sposób obsługi poczty elektronicznej,
c. Obsługa najnowszych funkcji Outlook 2013, 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,
d. Współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich

produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy.

e. Bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

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, wiadomości błyskawicznych i SMS-ów.
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 Internet Explorer, Apple Safari i Mozilla Firefox.

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

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych,
2. Zarządzanie strukturą portalu i treściami www,
3. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
4. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej,
5. Tworzenie repozytoriów wzorów dokumentów,
6. Tworzenie repozytoriów dokumentów,
7. Wspólną, bezpieczną pracę nad dokumentami,
8. Wersjonowanie dokumentów (dla wersji roboczych),
9. Organizację pracy grupowej,
10. Wyszukiwanie treści,
11. Dostęp do danych w relacyjnych bazach danych,
12. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

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

1. Interfejs użytkownika:
   a. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
   b. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0
   c. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
   d. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
   e. 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.
   g. Wbudowane samoobsługowe narzędzia wyszukiwania, analizy i wizualizacji danych Typu BI wraz z raportowaniem.

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 2010 i 2016z zapewnieniem konwersji wszystkich elementów i atrybutów dokumentu
m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

5. Arkusz kalkulacyjny musi umożliwiać:
   a. Tworzenie raportów tabelarycznych
   b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
   c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d. Wyszukiwanie i zamianę danych
   e. Wykonywanie analiz danych przy użyciu formatowania warunkowego
   f. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   g. Formatowanie czasu, daty i wartości finansowych z polskim formatem
   h. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   i. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
   j. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
6. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   a. Przygotowywanie prezentacji multimedialnych, które będą:
   b. Prezentowanie przy użyciu projektora multimedialnego
   c. Drukowanie w formacie umożliwiającym robienie notatek
   d. Zapisanie jako prezentacja tylko do odczytu.
   e. Nagrywanie narracji i dołączanie jej do prezentacji
   f. Opatrywanie slajdów notatkami dla prezentera
   g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
   h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
   i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
   j. Możliwość tworzenia animacji obiektów i całych slajdów
   k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
   l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.

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

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

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

a. Wymianę informacji z możliwością wyboru i zmiany dostępnego kanału komunikacji, tj. wiadomości tekstowych (chat), rozmowy (przekazywanie dźwięku), wideo rozmowy (przekazywanie dźwięku i obrazu), współdzielenie lokalnych pulpitów w systemach Windows oraz współdzielenie dokumentów z możliwością przejmowania kontroli i edycji przez uprawnionych uczestników.

2. Kontakt poprzez wymienione kanały w modelu jeden do jednego, jeden do wielu, telekonferencji (kontakt interakcyjny wielu osób) oraz udostępniania dźwięku i obrazu dla wielu osób w sieci intranet lub internet.
3. Możliwość oceny jakości komunikacji głosowej i wideo.
4. Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze katalogowej oraz definiowania opisów użytkowników zewnętrznych w tym użytkowników wybranych bezpłatnych komunikatorów i użytkowników sieci telefonii przewodowej i komórkowej.
5. Dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką SKW lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub specjalizowanych urządzeń stacjonarnych typu telefon IP, kamera dookólna, czy duże monitory lub projektory.
6. Dostępny kliencki sprzęt peryferyjny różnych producentów posiadający potwierdzenie zgodności z SKW przez producenta SKW.
7. Dostępność informacji o statusie dostępności użytkowników na liście adresowej (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności, w tym składowanych w usłudze katalogowej.
8. Możliwość grupowania kontaktów w komunikacji tekstowej z możliwością konwersacji typu jeden-do-jednego, jeden-do-wielu i możliwością rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat.
9. Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.
10. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.
11. Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
12. Możliwość nagrywania telekonferencji przez uczestników.
13. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
14. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
15. Wbudowane funkcjonalności: SIP Proxy.
16. Wbudowana funkcjonalność mostka konferencyjnego MCU.
17. Obsługa standardów: CSTA, TLS, SIP over TCP.
18. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
19. Kodowanie video H.264,
20. Wsparcie dla adresacji IPv4 i IPv6,
21. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
22. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników,
23. Możliwość szyfrowania połączeń.
24. Dostępność uczestniczenia w telekonferencjach poprzez przeglądarkę dla użytkowników z poza organizacji, zaproszonych do udziału w telekonferencji z funkcjami:
    a. Dołączania do telekonferencji,
    b. Szczegółowej listy uczestników
    c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
    d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
    e. Dostępu do udostępnianych plików,
    f. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji,
25. Dostępność aplikacji klienckiej usługi SKW (komunikatora) z funkcjonalnością:
    a. Listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielania grup kontaktów typu ulubione lub ostatnie.
    b. Historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
    c. Wsparcia telekonferencji:
    d. Dołączania do telekonferencji,
    e. Szczegółowej listy uczestników,
    f. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,

g. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
h. Głosowania,
i. Udostępniania plików i pulpitów,
j. Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,

26. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
27. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

Wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji SKW z wybranymi systemami poczty elektronicznej i portali intranet/internet oraz usługą katalogową Active Directory.
Wynikiem takiej integracji mają być następujące funkcje i cechy systemu opartego o SKW dostępne dla użytkowników posiadających odpowiednie uprawnienia licencyjne i nadane przez administratorów:

1. Wykorzystanie domenowego mechanizmu uwierzytelnienia w oparciu o usługę katalogową, jej profile użytkowników i ich grup oraz realizację fizyczną pojedynczego logowania (single sign-on) dla uprawnionego dostępu do usług SKW.
2. Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).
3. Współdziałanie mechanizmów SKW z pocztą głosowa, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:
    a. Uruchamiania funkcji komunikacyjnych SKW z wybranych interfejsów klienta poczty elektronicznej, składników pakietu biurowego czy portalu,
    b. Dostępności w tych interfejsach danych o statusie obecności innych użytkowników (np. w nagłówkach poczty elektronicznej, czy listach użytkowników portalu.
    c. Możliwość planowania rozmów czy telekonferencji bezpośrednio poprzez zaproszenia w kalendarzu klienta poczty elektronicznej, generujące link do spotkania on-line.

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

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

Usługi bezpieczeństwa wbudowane w Produkt muszą pozwalać na:

1. Zarządzanie prawami dostępu do dokumentów i poczty elektronicznej tworzonych w Usłudze poprzez ich szyfrowanie i nadawanie praw odczytu, edycji, wydruku dla konkretnych użytkowników Usługi lub grup użytkowników Usługi.
2. Wykrywanie słów kluczowych w przesyłanych wiadomościach i sygnalizowanie potencjalnego wycieku informacji.
3. Możliwość ograniczania przedziału czasowego uprawnionego dostępu użytkowników do informacji.
4. Możliwość stosowania wymogu wieloskładnikowego uwierzytelniania.

Usługi analizy danych wbudowane w Produkt muszą umożliwiać:

1. Konfigurowanie on-line kokpitów informacyjnych wizualizujących wyniki analiz danych.
2. Gotowe mechanizmy podłączania różnego rodzaju danych strukturalnych, semi-strukturalnych i niestrukturalnych.
3. Korzystanie z gotowych algorytmów i modeli analizy oraz budowa własnych modeli w języku R.

Subskrypcja pakietu biurowego
Usługa hostowana on-line musi zawierać subskrypcję pakietu biurowego spełniającego następujące wymagania:
Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit,
2. Wymagania odnośnie interfejsu użytkownika:

a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
4. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
5. 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,
6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
8. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
10. 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.
11. 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 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
p. Zapis i edycję plików w formacie PDF.
q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco,
s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.

12. 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 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
    q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

13. 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 2010, 2013 i 2016.

14. 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.
15. 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.
16. 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.
17. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
    a. Pełna polska wersja językowa interfejsu użytkownika.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Dostępność aplikacji na platformie Windows 7 lub wyższych oraz OSX 10 lub wyższych,

d. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
e. Możliwość obsługi tekstowych wiadomości błyskawicznych w modelu jeden do jeden i jeden do wielu.
f. Możliwość komunikacji głosowej i video w modelu jeden do jeden i jeden do wielu.
g. Obsługa telekonferencji SKW:
    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 specjalizowanych urządzeń peryferyjnych zgodnych z SKW.
o. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
p. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
q. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Subskrypcja usługi zarządzania urządzeniami oraz tożsamością użytkowników

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

a. Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy,
b. Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym),
c. Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm, w tym zgodności z normami ISO 27017 i 27018,
d. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO.
e. Możliwość skalowania usługi z ustalonymi kosztami takiego skalowania,

f. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
g. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
h. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
i. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
j. Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione".
k. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
l. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
m. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
n. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych,
o. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Unii Europejskiej.
p. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
q. Mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.
r. Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.
s. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.

Wymagania funkcjonalne

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

Wymagane scenariusze użycia:

1. Automatyczna klasyfikacja treści dokumentów (przechowywanych na zasobach plikowych, bibliotekach lub transportowanych poprzez system pocztowy) zgodnie z definiowanymi wzorcami,
2. Wykorzystanie klasyfikacji danych do dynamicznego aplikowanie restrykcji związanych z dostępem do informacji zapobiegające niekontrolowanemu wyciekowi informacji,
3. Bezpieczna wymiana plików wewnątrz organizacji oraz z zewnętrznymi odbiorcami niezależnie od typu pliku, posiadanego urządzenia (PC lub urządzenie mobilne Windows Phone, Android, iOS) lub przynależności do organizacji, umożliwiające granularną kontrolę dostępu do poufnych informacji i wymuszenie ustalonych polityk ochrony informacji,
4. Możliwość wykorzystania telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS lub specjalizowanych aplikacji, potwierdzających tożsamość użytkownika podczas dostępu do aplikacji webowych pozwalające na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia, lub z poza sieci lokalnej,
5. Możliwość pracy na prywatnych urządzeniach użytkowników zapewniający bezpieczny i kontrolowany dostęp do danych i aplikacji, w możliwością wydzielenia i usunięcia danych służbowych z urządzenia,

6. Jednokrotne logowanie (single sign-on)w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika, przy zachowaniu niezaprzeczalności działań,
7. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwalający na redukcję ilości zgłoszeń działów wsparcia,
8. Automatyczne przepływy pracy i reguł biznesowych pozwalające przyspieszenie procesów i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie ustalonych polityk i procedur),
9. Ochrona danych poprzez wykrywanie i mapowanie ról biznesowych pozwalające na audyt i kontrolę zgodności realizacji uprawnień użytkowników z ustalonymi politykami oraz ciągłą weryfikację stanu bezpieczeństwa systemów.
10. Zarządzanie urządzeniami mobilnymi pozwalające na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwiające zdalne kasowanie danych firmowych lub całego urządzenia.

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

1. System zarządzania tożsamością musi umożliwiać zastosowanie - przy połączeniu ze źródłami danych - mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji).
2. System musi zapewniać prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej zaporami *firewall* oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
3. System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
4. System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.

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

Interoperacyjność

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

Skalowalność funkcjonalna

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

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

Wymagania w zakresie cech i funkcjonalności rozwiązania

1. Agregacja i synchronizacja danych

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

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

c. System musi zapewniać możliwość komunikacji z powyższymi informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
d. System musi zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy integrujące poprzez budowę odpowiedniego rozszerzenia systemu.
e. System musi zapewniać możliwość uprawnionego tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.
f. System musi dostarczać mechanizmy pozwalające na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
g. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system musi umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium, umożliwiając synchronizację danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
h. System musi oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
i. System musi umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.

2. Repozytorium danych teleadresowych
   a. System musi umożliwiać agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.
   b. System misi zapewnić interfejs użytkownika zapewniający możliwość wyszukiwania oraz przeglądania danych dla wszystkich uprawnionych użytkowników systemu.
   c. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie dostępu, zarządzania oraz uaktualnienia danych teleadresowych.
   d. W ramach interfejsu użytkownika system musi zapewniać możliwość udostępnienia edycji zakresu udostępnianych danych samodzielnie przez każdego z uprawnionych użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.
3. Zarządzanie kartą elektroniczną
   a. Zarządzanie kartami elektronicznymi musi obejmować: personalizację graficzną kart (nadruk), zdalne zarządzania PIN'ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów),
   b. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 10 000 użytkowników,
   c. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnym przechowywanym i wygenerowanym na karcie)
   d. System musi umożliwiać wydawanie i zarządzanie wieloma certyfikatami na jednej karcie (przewiduje się wykorzystanie 4 certyfikatów dla jednego użytkownika)
   e. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania itp.,
   f. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP,

g. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI,
h. System musi wspierać zarządzanie certyfikatami używanymi do uwierzytelnienia w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.
i. System musi umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów,
j. Po wystawieniu certyfikatu, system musi umożliwić włączenie automatycznej publikacji certyfikatu w katalogu LDAP,
k. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP,
l. Certyfikaty wystawione na jednej stacji muszą być automatycznie dostępne dla użytkownika na innej stacji o ile się tam zaloguje (dotyczy certyfikatów przechowywanych w profilu użytkownika jak i certyfikatów przechowywanych na karcie elektronicznej),
m. Systemu musi posiadać przyjazny interfejs oparty o WWW, przez który użytkownik końcowy może wykonywać operacje zarządzania swoimi certyfikatami i PIN'ami dostępowymi (zmiana PIN'u, odblokowanie karty),
n. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/ wygenerowanie PIN'u inicjującego do karty elektronicznej następującymi drogami:
- Użytkownik lub administrator wprowadza PIN inicjujący,
- PIN inicjujący jest losowo generowany przez system i przekazywany użytkownikowi po autoryzacji na stronie WWW,
- System generuje PIN inicjujący i drukuje go w sposób uniemożliwiający odczytanie go przez osoby postronne bez rozerwania koperty / wydruku,
- PIN może być dostarczony do systemu z zewnętrznego źródła (musi być dostarczone odpowiednie API),

o. Personalizacją graficzna musi pobierać ze wskazanego przez Zamawiającego źródła danych, zdjęcia pracowników i umieszczać je wraz z innymi danymi identyfikacyjnymi na karcie.
p. System musi umożliwiać odblokowanie kart w oparciu o autoryzację użytkownika w katalogu LDAP z wykorzystaniem hasła jednokrotnego,
q. Bezpośrednie odblokowanie karty musi być wykonywane w oparciu mechanizm challenge/response (zabrania stosowania się SO PIN'u statycznego),
r. Na PIN'y wykorzystywane przez użytkownika musi być możliwość nakładania polityk bezpieczeństwa definiujących stopień skomplikowania PIN'u, w szczególności:
- nie mniej niż 6 znaków,
- wymagane cyfry litery małe i duże,
- PIN może się powtarzać przez N zmian,

s. System musi wspierać karty Cryptotech MultiliSign 2.0 lub równoważne,
t. Zarządzanie wystawianiem certyfikatów musi się odbywać w oparciu o definiowalny przepływ roboczy (workflow), który będzie mógł być modyfikowany bezpośrednio przez operatora systemu z poziomu interfejsu graficznego,
u. Workflow musi umożliwiać, implementacji następujących scenariuszy użycia:
- w pełni automatyczne wystawianie certyfikatów dla użytkowników,
- wystawianie certyfikatów wymagające każdorazowej aprobaty operatora systemu,
- automatyczne odświeżanie wybranych certyfikatów,
- automatyczne odtwarzanie wszystkich certyfikatów na kartę elektroniczną w przypadku jej zastąpienia,
- weryfikację czy użytkownik ma odpowiednie certyfikaty lub czy certyfikaty nie wygasają i w razie potrzeby system musi uruchamiać odpowiednią procedurą wystawiania lub wznawiania certyfikatu,
- powiadamianie administratorów systemu o wygasaniu certyfikatów dla serwerów / urządzeń wchodzących w skład infrastruktury teleinformatycznej,

v. Wbudowane workflow musi udostępnić możliwość definiowanie wielu wzorców certyfikatów (w zależności od ich zastosowania) w połączeniu z odpowiednią ścieżką wystawiania/dostarczania certyfikatów do użytkownika, w szczególności:
- certyfikat do szyfrowania poczty wystawiany jest automatycznie o ile użytkownik posiada certyfikat na karcie elektronicznej do podpisu, podpis ten musi być użyty do podpisania wystawianie certyfikatu do szyfrowania,

- certyfikat do logowania jest wystawiony, jeśli użytkownik posiada kartę elektroniczną przypisaną do siebie oraz poprawnie zautoryzuje się hasłem jednokrotnym na stronie WWW systemu,

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

w. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, liczby zmian PIN'ow, czy liczby odblokowanych kart,
x. Dane służące do deszyfracji kluczy prywatnych użytkowników przechowywanych w systemie, muszą być bezpiecznie składowane na urządzeniu HSM typu nCipher netHSM 500 lub w pełni równoważnych,
y. Bezpośrednie zarządzania kartami musi odbywać się przez dostarczany wraz z systemem Microsoft Windows interfejs „Microsoft Smart Card Base CSP" lub standard PKCS#11,
z. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania).

Podsystem zarządzania urządzeniami mobilnymi

1. Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:
   a. Integrację z systemem Microsoft SCCM w oparciu o natywne interfejsy komunikacyjne
   b. Wykorzystanie bazy użytkowników znajdujących się w Active Directory
   c. Inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych,
   d. Inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji:
      – Nazwa urządzenia
      – Identyfikator urządzenia
      – Nazwa platformy systemu operacyjnego
      – Wersja oprogramowania układowego
      – Typ procesora
      – Model urządzenia
      – Producent urządzenia
      – Architektura procesora
      – Język urządzenia
      – Lista aplikacji zainstalowanych w ramach przedsiębiorstwa
2. W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).
3. Wymagania w zakresie dystrybucji oprogramowania:
   a. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
   b. Usługa ma umożliwiać dystrybucję oprogramowania na żądanie użytkownika, realizowane poprzez wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji
   c. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
   d. Katalog aplikacji ma wspierać następujące formaty aplikacji mobilnych:
      – *. appx (Windows RT)
      – *.xap (Windows Phone 8)
      – *.ipa (iOS)
      – *.apk (Android)

   e. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:

- Windows Store
- Windows Phone Store
- Android Google Play Store
- iOS App Store

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

Podsystem ochrony informacji

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

1. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,
2. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
3. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
4. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
5. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, w tym:
   a. Brak uprawnień dostępu do informacji,
   b. Informacja tylko do odczytu,
   c. Prawo do edycji informacji,
   d. Brak możliwości wykonania systemowego zrzutu ekranu,
   e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
   f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
   g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.
6. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
7. Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji,
8. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji,
9. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
10. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

Podsystem usługi katalogowej

Usługa katalogowa musi zapewnić:

1. Możliwość zintegrowania jednokrotnego logowania (SSO) dla popularnych aplikacji typu SaaS,
2. Gotowe mechanizmy uwierzytelniania do aplikacji webowych dla użytkowników zewnętrznych,
3. Możliwość połączenia lub synchronizacji z usługą Active Directory wewnątrz organizacji,
4. Scentralizowane zarządzanie przydzielania dostępu do aplikacji,
5. Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),
6. Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),
7. Samoobsługowe resetowania hasła,
8. Dostarczanie mechanizmów usługi katalogowej uwierzytelniania użytkowników,
9. Konsolę zarządzania tożsamością i dostępem.

Microsoft Office 365 E3 z Office 365 E1 step up Możliwość zamiany subskrypcji pakietu usług hostowanych typu I na pakiet usług hostowanych typu II w trakcie trwania umowy
Microsoft Office 365 E5 z Office 365 E3 step up Możliwość zamiany subskrypcji pakietu usług hostowanych typu II na pakiet usług hostowanych typu III w trakcie trwania umowy
Microsoft Office 365 E5 z Office 365 E1 step up Możliwość zamiany subskrypcji pakietu usług hostowanych typu I na pakiet usług hostowanych typu III w trakcie trwania umowy
Azure Monetary Commitment lub równoważny **Pakiet hostowanych usług platformowych - na jeden miesiąc**

Subskrypcja standardowej, powszechnie dostępnej przez internet platformowej usługi hostowanej typu COTS (Commercial Of-The-Shelf) polegająca na udostępnieniu skalowalnej platformy pozwalającej wykorzystać w formie usługi serwerowe systemy operacyjne, silniki baz danych oraz inne aplikacje w środowiskach zwirtualizowanych.
Usługa ta ma posiadać następujące parametry:

1. Udostępnienie skalowalnej platformy pozwalającej wykorzystać w formie usługi serwerowe systemy operacyjne, silniki baz danych oraz inne aplikacje w środowiskach zwirtualizowanych.
2. Dostępność usługi w okresie trwania umowy gwarantująca na jeden miesiąc zasoby:
    a. Minimum 1 jednostka obliczeniowa o parametrach 1 rdzeń procesora, 1,7GB RAM, pod kontrolą systemu operacyjnego Windows Server lub Linux (wybrane dystrybucje), w okresie dostępności usługi,
    b. Minimum 70 GB dostępnej lokalnie redundantnej przestrzeni dyskowej,
    c. Minimum 70 GB dostępnej georedundantnej przestrzeni dyskowej (odległości min. 200km między lokalizacjami),
    d. Minimum 100 GB transferu danych do i z platformy usługi hostowanej.
3. Gwarantowana dostępność usług platformy na poziomie 99,9%,
4. Dostępny portal administracyjny, pozwalający na uruchamianie poprzez wybór dostępnych usług platformy.
5. Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci).
6. Możliwość wyboru różnych rodzajów dysków i ich pojemności.
7. Możliwość uruchomienia aplikacji internetowych wykorzystujących technologię ASP.NET, PHP, Java, Python z automatyczną dystrybucją ruchu sieciowego HTTP pomiędzy kilka pracujących serwerów.
8. Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów z możliwością zdalnego dostępu.
9. Możliwość analizy danych gromadzonych w czasie rzeczywistym i danych historycznych.
10. Komunikacja z usługą poprzez REST API.
11. Zbieranie danych operacyjnych z wykorzystaniem dedykowanego oprogramowania – agenta,
12. Kompatybilność w zakresie monitorowania i zarządzania z Microsoft System Center Operations Manager,
13. Narzędzia tworzenia aplikacji mobilnych spełniające następujące wymagania (opcjonalnie dostępnych w ramach usługi):
    a. Wsparcie dla urządzeń z systemem klienckim Windows, Windows Phone, iOS, Android oraz HTML5
    b. Wsparcie po stronie platformy dla JavaScript i .Net
    c. Integracja z serwisami notyfikacji i uwierzytelniania
    d. Obsługa wysyłania poczty elektronicznej email
    e. Obsługa skryptów i zadań wg harmonogramu
    f. Możliwość gromadzenia logów i monitorowania usługi.
14. 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

15. 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.
16. Dostępność relacyjnej i nierelacyjnej bazy danych, w tym oparte o technologię Hadoop, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
17. Możliwość zestawienia dedykowanego łącza pomiędzy siedzibą Zamawiającego a dostawcą Platformy w technologii MPLS.
18. Możliwość dostarczenia dedykowanego urządzenia stanowiącego lokalny magazyn przechowywania danych, podłączony do chmury z funkcją deduplikacji, szyfrowania i hierarchizacji pamięci, objętego wsparciem dostawcy Platformy.
19. 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.

Przewidywalny koszt budowy i utrzymania

1. Oparcie się o usługi typu subskrypcji standardowej, powszechnie dostępnej przez internet platformowej 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 platformy.
3. Możliwość zmiany wymaganych parametrów usługi i jej skalowania zgodnie z potrzebami.
4. Możliwość automatycznego skalowania mocy obliczeniowej platformy.
5. Płatność za fizyczne wykorzystanie usług platformy z możliwością ich okresowego wyłączania.

Zgodność ze standardami

1. Dostępność narzędzi wspomagających migrację aplikacji i danych zarówno ze środowisk własnych do Platformy, jak i z Platformy na dowolną inną platformę opartą o standard serwerów X64, a więc pozwalających na przeniesienie usług w przypadku podjęcia takiej decyzji.
2. Zastosowanie w Platformie powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy, w szczególności:

- ISO 27001, ISO 27002, ISO 27017, ISO 27018
- UK G-Cloud
- SOC 1, SOC 2
- TDS (tabular data stream)
- Open Authentication Standard – OAuth
- OData

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 Platformy dla standardowych rozwiązań OpenSource takich jak WordPress, Joomla, Drupal, OrchardCMS, MediaWiki, phpBB czy Mojo. Dostępność w ramach platformy predefiniowanych obrazów z tym oprogramowaniem.

Dostępność systemów i ich bezpieczeństwo

1. Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym),
2. Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy.

3. 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.
4. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
5. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
6. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
7. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
8. Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
9. 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".
10. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
11. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN)
12. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
13. Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km.

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 Europejskiego Obszaru Gospodarczego.
3. Zobowiązania umowne potwierdzające zgodność z rozp. RODO i potwierdzające rolę operatora usługi jako współprzetwarzającego dane,
4. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
5. Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.
6. Gwarancja usunięcia danych Zamawiającego z Platformy po zakończeniu umowy.
7. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy Platformy.
8. Gwarancja usunięcia danych w terminie 180 dni od wygaśnięcia subskrypcji i zakończenia umowy.

Microsoft Premier Professional Enterprice Service lub równoważny **Pakiet usług wsparcia technicznego – pakiet roczny**

Pakiet usług wsparcia technicznego musi obejmować swoim zakresem świadczenie opieki serwisowej oprogramowania i usług producenta oferowanych produktów w okresie trwania subskrypcji.
W wymaganiach zastosowano następujące definicje:

1. Podstawowe Godziny Wsparcia – dni robocze od godz. 09:00 do godz. 17:00, czasu środkowoeuropejskiego.
2. Pozostałe Godziny Wsparcia – dni robocze od godz. 17:00 do godz. 09:00 dnia następnego, niedziele i święta określone w przepisach o dniach wolnych od pracy.
3. Czas Reakcji – maksymalny czas pomiędzy zgłoszeniem problemu a przystąpieniem do analizy Problemu i poszukiwania rozwiązania.
4. Czas Reakcji „on-site" – czas pomiędzy potwierdzeniem przyjęcia zgłoszenia a pojawieniem się Inżyniera Wsparcia na miejscu w siedzibie Zamawiającego.
5. Waga Problemu – miara ważności Problemu ustalana przez Zamawiającego:
    a. Problem **krytyczny** - mający krytyczny wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe krytyczne dla działalności biznesowej Zamawiającego przestały funkcjonować i potrzebna jest natychmiastowa pomoc.
    b. Problem **poważny** - mający poważny wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe Zamawiającego funkcjonują w sposób poważnie utrudniający

normalną pracę lub nie funkcjonują w ogóle – potrzebna jest pomoc nie później niż w czasie 1 godziny od zgłoszenia problemu.

c. Problem **umiarkowany** - mający umiarkowany wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe Zamawiającego funkcjonują w sposób utrudniający normalną pracę – potrzebna jest pomoc nie później niż w czasie 2 godzin od zgłoszenia problemu.

d. Problem **minimalny** - mający minimalny wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe Zamawiającego funkcjonują poprawnie, aczkolwiek występują pewne drugorzędne i prawie niezauważalne trudności – potrzebna jest pomoc ze nie później niż w czasie 4 godzin od zgłoszenia Problemu.

Dla problemów umiarkowanych i minimalnych w okresie tzw. Pozostałych Godzin Wsparcia nie jest wymagany ustalony czas reakcji.

1. Wymagana jest dostawa subskrypcji pakietu wsparcia technicznego, który zapewni:
   a. Świadczenie usługi w zakresie organizacji i koordynacji usług w zakresie wsparcia technicznego oprogramowania wyprodukowanego przez Microsoft, w odniesieniu do którego nie zakończył się okres tzw. dodatkowego wsparcia.
   b. Usługi w zakresie wsparcia technicznego świadczone przez okres 36 miesięcy od dnia podpisania umowy.
   c. Zapewni możliwość bezpośredniego zgłaszania problemów technicznych do producenta oprogramowania lub spółki zależnej producenta (Producenta) drogą elektroniczną poprzez dedykowaną stronę Producenta i telefonicznie.
   d. Zagwarantuje możliwość wykonywania poprawek do oprogramowania (HotFix) przez Producenta.
2. Warunki świadczenia usług w zakresie wsparcia technicznego Produktów:
   a. Usługi w zakresie wsparcia technicznego (Produktów) mają obejmować świadczenie Zamawiającemu przez certyfikowanych specjalistów, pracowników Producenta, pomocy przy rozwiązywaniu problemów dotyczących Produktów, które pojawiły się u Zamawiającego przy korzystaniu z takich Produktów, jeżeli zachodzi uzasadnione podejrzenie, że taki problem został spowodowany przez Produkty (w szczególności, z możliwością tworzenia poprawek z wykorzystaniem dostępu do kodu źródłowego Produktów).
   b. Wymagane jest świadczenie usług mających na celu efektywne i skuteczne zapobieganie problemom dotyczącym Produktów polegające w szczególności na okresowych spotkaniach z certyfikowanymi specjalistami Producenta Produktów i przygotowywaniu odpowiednich raportów, uzyskaniu dostępu do poprawek do Produktów czy zasobów Producenta z artykułami i wskazówkami dotyczącymi rozwiązywania i zapobiegania Problemom.
   c. Zamawiający ma uzyskać priorytetowy dostęp, przez zapewnienie dedykowanego numeru telefonicznego i internetowego dostępu technicznego do certyfikowanych specjalistów Producenta w celu szybkiego zgłaszania problemów dotyczących Produktów oraz uzyskiwania wsparcia.
   d. W ramach usług wsparcia technicznego Zamawiający wymaga przedstawienia oferty na standardowe pakiety wsparcia technicznego zawierające 100godzin roboczych możliwych do wykorzystania w okresie 12 miesięcy.
   e. Zamawiający wymaga możliwości konwersji incydentów pomocy technicznej dostępnych w ramach obecnie obowiązujących oraz podpisanych w okresie obowiązywania umowy wsparcia technicznego umów licencyjnych, na godziny wsparcia technicznego świadczonego w ramach pakietów usług wsparcia technicznego, w wymiarze do 140 godzin dla jednego pakietu.
   f. Wymagane jest umożliwienie wsparcia technicznego dla Produktów wychodzących z okresu tzw. wsparcia rozszerzonego, to znaczy dla Produktów, które na podstawie innych umów nie są objęte wsparciem Producenta.
   g. Usługi w zakresie wsparcia technicznego Produktów powinny być dostępne przez 24 godziny na dobę i 7 dni w tygodniu. Zgłoszenia problemów będą dokonywane bezpośrednio do Producenta na dedykowany numer telefoniczny (dla wszystkich zgłoszeń) lub zgłaszane w formie elektronicznej na dedykowanym serwisie internetowym (dla zgłoszeń umiarkowanych i minimalnych), do certyfikowanych specjalistów Producenta. Termin rozpoczęcia prac nad zgłoszonym problemem objętym usługami w zakresie wsparcia technicznego Produktów przez takich specjalistów (tzw. czas reakcji) powinien zależeć od wagi zgłaszanego problemu:

- Problemy **krytyczne i poważne** - czas reakcji telefonicznej do jednej godziny w trybie 24 godziny na dobę i 7 dni w tygodniu;
- Problemy **umiarkowane** - czas reakcji 2 godziny w godzinach 9-17 od poniedziałku do piątku z wyłączeniem, świąt i dni wolnych od pracy na podstawie przepisów prawa;
- Problemy **minimalne** - czas reakcji 4 godziny w godzinach 9-17 od poniedziałku do piątku z wyłączeniem, świąt i dni wolnych od pracy na podstawie przepisów prawa.

h. W ramach usług w zakresie wsparcia technicznego Produktów będzie istniała możliwość świadczenia takich usług na miejscu w lokalizacji Zamawiającego w Polsce (tzw. usługi wsparcia „on-site"). Usługi świadczone w lokalizacji Zamawiającego w Polsce będą rozliczane w ramach dostępnej dla Zamawiającego puli godzin usług, o których mowa w pkt. 3.1 powyżej.

i. Pakiet usług zapewni regularne przekazywanie Zamawiającemu przez Producenta informacji technicznych w postaci biuletynu technicznego osobom kontaktowym wskazanym przez Zamawiającego.

j. W ramach usług w zakresie usług wsparcia technicznego do Zamawiającego zostanie przypisany dedykowany specjalista Producenta, który będzie odpowiedzialny za realizację usług w zakresie wsparcia technicznego dla Zamawiającego, a także za przekazywanie oraz otrzymywanie informacji i komentarzy zwrotnych dotyczących świadczonych usług. Jednocześnie Zamawiający w terminie do 14 dni od daty podpisania umowy wyznaczy ze swojej strony osoby (w tym koordynatora wsparcia technicznego) uprawnione do składania u specjalisty Producenta zgłoszeń w ramach usług w zakresie wsparcia technicznego Produktów.

k. Po podpisaniu umowy w zakresie usług wsparcia technicznego, w uzgodnionym terminie, przedstawiciel Producenta przeprowadzi sesję orientacyjno-przeglądową u Zamawiającego. Sesja może być przeprowadzona telefonicznie lub w lokalizacji Zamawiającego. Celem takiej sesji jest szczegółowe omówienie dostępnych usług w zakresie wsparcia technicznego, zasad ich świadczenia, zebranie informacji o potrzebach Zamawiającego w zakresie wsparcia oraz opracowanie planu współpracy obejmującego okres świadczenia usług wsparcia technicznego, który będzie dokumentem roboczym, przeglądanym i uaktualnianym przez strony w regularnych odstępach czasu i który będzie obejmował wiedzę na temat planowanych i aktualnych działań w stosunku do Zamawiającego, jak również usług wykonanych w przeszłości.

Wymagany sposób realizacji usług w przypadku wystąpienia problemu:

Waga Problemu	Sytuacja	Oczekiwana Reakcja	Oczekiwana Reakcja Klienta
1 wyłącznie zgłoszenie telefoniczne	• Katastrofalny wpływ na działalność: • Podstawowe procesy biznesowe (mission critical) przestały funkcjonować i nie można w rozsądny sposób kontynuować pracy • Konieczna natychmiastowa pomoc	• Odpowiedź na pierwszy telefon w czasie nie dłuższym niż 1 godzina • Pracownicy Producenta wysłani do lokalizacji Klienta tak szybko, jak to będzie możliwe • Praca w systemie 24 godziny przez 7 dni w tygodniu • Błyskawiczna eskalacja do zespołów Produktowych Producenta • Powiadomienie kierownictwa wyższego szczebla Producenta	• Powiadomienie kierownictwa wyższego szczebla Klienta • Przydzielenie odpowiednich zasobów w celu umożliwienia prowadzenia prac w systemie 24 godziny przez 7 dni w tygodniu • Szybki dostęp i czas reakcji władz kontrolujących zmiany
A Wyłącznie zgłoszenie telefoniczne	• Krytyczny wpływ na działalność: • Znacząca utrata lub obniżenie jakości usług • Wymaga pomocy w ciągu 1 godziny	• Odpowiedź na pierwszy telefon w czasie nie dłuższym niż 1 godzina • Pracownicy Producenta wysłani do lokalizacji Klienta tak szybko, jak to będzie możliwe • Prace w systemie 24 godziny przez 7 dni w tygodniu • Powiadomienie kierownictwa Producenta wyższego szczebla	• Przydzielenie odpowiednich zasobów w celu umożliwienia prowadzenia prac w systemie 24 godziny przez 7 dni w tygodniu • Szybki dostęp i czas reakcji władz kontrolujących zmiany • Powiadomienie kierownictwa
B Zgłoszenie telefonicznie lub za pośrednictwem Internetu	• Umiarkowany wpływ na działalność: • Umiarkowana utrata lub obniżenie jakości usług, jednakże praca może być kontynuowana bez zakłóceń • Wymaga pomocy w ciągu 2 Godzin Roboczych	• Odpowiedź na pierwszy telefon w czasie nie dłuższym niż 2 godziny • Prace realizowane wyłącznie w Godzinach Roboczych	• Przydzielenie odpowiednich zasobów w celu umożliwienia prowadzenia ciągłych prac w Godzinach Roboczych[1] • Dostęp i reakcja władz kontrolujących zmiany w ciągu 4 Godzin Roboczych
C Zgłoszenie telefonicznie lub za pośrednictwem Internetu	• Minimalny wpływ na działalność: • Działalność prowadzona praktycznie z niewielkimi zakłóceniami lub bez zakłóceń • Wymaga pomocy w ciągu 4 Godzin Roboczych	• Odpowiedź na pierwszy telefon w czasie nie dłuższym niż 4 godziny • Prace realizowane wyłącznie w Godzinach Roboczych	• Podanie dokładnych informacji kontaktowych • Reakcja w ciągu 24 godzin.

3. Porady Techniczne:

Porady Techniczne muszą obejmować krótkoterminowe udzielanie porad i wskazówek w związku z problemami nieobjętymi Usługami Wsparcia Technicznego. Do Porad Technicznych zalicza się również krótkoterminowe usługi konsultacyjne dotyczące kwestii związanych z projektowaniem, rozwojem i wdrożeniami. Pracownik Producenta podejmie współpracę z Zamawiającym w celu określenia indywidualnych potrzeb Klienta w zakresie Porad Technicznych.
Następujące Porady Techniczne mogą być wykorzystane na podstawie niniejszego Opisu Usług:

1) Porady dotyczące Infrastruktury. Porady dotyczące Infrastruktury obejmują udzielanie nieformalnych porad, wskazówek i przekazywanie wiedzy w celu umożliwienia Zamawiającemu wdrożenia technologii Producenta w sposób pozwalający uniknąć powszechnych trudności technicznych i zmniejszyć ryzyko wystąpienia nieprzewidzianych awarii i przestojów w pracy systemów.

Usługi te pomagają Zamawiającemu także w rozwiązywaniu problemów niezwiązanych z Produktami, w tym:

- Błędów spowodowanych przez infrastrukturę sieciową Zamawiającego, sprzęt, oprogramowanie innych dostawców, procedury operacyjne, architekturę, procesy zarządzania usługami IT, konfigurację systemu lub błędy ludzkie.
- Problemów związanych ze zgodnością i koordynacją produktów wielu dostawców. Na żądanie Zamawiającego Wykonawca nawiąże współpracę z dostawcami oprogramowania będącymi osobami trzecimi w celu rozwiązania złożonych problemów związanych z brakiem zgodności produktów różnych dostawców.

2) Analizy. Analiza ma być oceną określonego systemu, aplikacji lub architektury mającą na celu ustalenie kwestii związanych z projektowaniem, rozwojem, wdrożeniem oraz możliwością wsparcia technicznego w odniesieniu do dotychczasowych lub planowanych wdrożeń technologii Producenta. Zakres każdej analizy będzie ustalany indywidualnie oraz oszacowany przed przydzieleniem zasobów. Efektem analizy ma być sporządzenie pisemnego raportu celem udokumentowania ustaleń i zaleceń.
3) Wsparcie dla Programistów. Wsparcie dla Programistów ma zapewnić Zamawiającemu opracowywanie i rozwijanie wewnętrznych aplikacji na platformach Producenta. Wsparcie dla Programistów obejmuje przede wszystkim narzędzia programistyczne i technologie Producenta.
4) Dostęp do Laboratorium. Zamawiający wymaga możliwości zapewnienia dostępu do laboratorium w ramach pomocy dotyczącej opracowywania produktu, testowania, przygotowywania wersji wstępnych oraz działań migracyjnych Produktów.

4. Usługi Informacyjne.

W ramach Usług Informacyjnych Zamawiający wymaga dostępu do informacji technicznych na temat Produktów oraz narzędzi wsparcia, które mają za zadanie pomóc w efektywnym i skutecznym wdrożeniu oraz używaniu Produktów. Usługi Informacyjne mają obejmować dowolne połączenie poniższych usług:

a. Witryna sieciowa zapewniająca bezpłatny dostęp do następujących zasobów informacyjnych:

- Regularnie aktualizowane informacje o produktach zawierające kluczowe informacje na temat wsparcia i obsługi Produktów.
- Ostrzeżenia informujące Zamawiającego o potencjalnie poważnych problemach.

b. Aplikacja internetowa umożliwiająca zgłaszanie i sprawdzanie statusu zgłoszonych Incydentów.

- Baza wiedzy Producenta zawierająca artykuły techniczne i narzędzia oraz wskazówki dotyczące rozwiązywania problemów.

c. Transmisje dot. Wsparcia. Transmisje dot. wsparcia mają zapewnić regularnie odbywające się dyskusje „na żywo” za pośrednictwem Internetu, prowadzone przez kierowników programowych Producenta, programistów i ekspertów głównie na tematy związane z technologiami Producenta.

Microsoft Premier Professional Enterprice Service AddOn lub równoważny **Pakiet godzin uzupełniających do pakietu usług wsparcia technicznego – 20 godzin wsparcia**

Pakiet dodatkowych godzin wsparcia technicznego jest rozszerzeniem zakresu usług zawartych w opisanym w SIWZ Pakiecie Usług Wsparcia Technicznego.
Usługi te realizowane mają być jako w sposób zawarty w opisie Pakietu Usług wsparcia technicznego.
Pakiet dodatkowych godzin wsparcia technicznego ma gwarantować Zamawiającemu na wyżej opisanych zasadach dodatkowe 20 godzin roboczych usług.

Microsoft Office Standard 2019 lub równoważny **Pakiet biurowy**

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.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
3. 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 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. Pozwala zapisywać dokumenty w formacie XML.
4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego.
5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.
7. 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 zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
    f. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
8. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b. Wstawianie oraz formatowanie tabel.
    c. Wstawianie oraz formatowanie obiektów graficznych.
    d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    f. Automatyczne tworzenie spisów treści.
    g. Formatowanie nagłówków i stopek stron.
    h. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
    i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
    j. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.
    k. Wydruk dokumentów.
    l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
    m. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
    n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
p. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

9. Arkusz kalkulacyjny musi umożliwiać:
   a. Tworzenie raportów tabelarycznych
   b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
   c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
   e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
   f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
   g. Wyszukiwanie i zamianę danych
   h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
   i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
   k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
   l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   m. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
   n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
10. 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 2007, MS PowerPoint 2010, 2013 i 2016.
11. 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.

12. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
    a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
    b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
    c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
    d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
    e. Automatyczne grupowanie wiadomości poczty o tym samym tytule,
    f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
    g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
    h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
    i. Zarządzanie kalendarzem,
    j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
    k. Przeglądanie kalendarza innych użytkowników,
    l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
    m. Zarządzanie listą zadań,
    n. Zlecanie zadań innym użytkownikom,
    o. Zarządzanie listą kontaktów,
    p. Udostępnianie listy kontaktów innym użytkownikom,
    q. Przeglądanie listy kontaktów innych użytkowników,
    r. Możliwość przesyłania kontaktów innym użytkowników,
    s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.