Numer sprawy: GDDKiA-DII-WEiPI-dn-2812-5/14

GENERALNA DYREKCJA DRÓG KRAJOWYCH I AUTOSTRAD

ul. Wronia 53

00-874 Warszawa

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA DO PRZETARGU NIEOGRANICZONEGO O WARTOŚCI POWYŻEJ 134.000 EURO NA DOSTAWĘ DLA GDDKiA NOWYCH LICENCJI, AKTUALIZACJĘ JUŻ UŻYTKOWANYCH LICENCJI ORAZ WSPARCIE TECHNICZNE I OPIEKĘ SERWISOWĄ

Specyfikacja Istotnych Warunków Zamówienia zawiera:

Z A T W I E R D Z A M

DYREKTOR GENERALNY

Joanna Nurkiewicz

Warszawa, 1 kwietnia 2014 r.

Rozdział I

Instrukcja dla Wykonawców

1. ZAMAWIAJĄCY

Generalna Dyrekcja Dróg Krajowych i Autostrad
00-874 Warszawa, ul. Wronia 53
telefon: 0-22 375 86 67, faks 0-22 375 86-21

2. OZNACZENIE POSTĘPOWANIA

Postępowanie, którego dotyczy niniejszy dokument oznaczone jest znakiem: **GDDKiA-DII-WEiPI-dn-2812-5/14**
Wykonawcy winni we wszelkich kontaktach z Zamawiającym powoływać się na wyżej podane oznaczenie.

3. TRYB POSTĘPOWANIA

Postępowanie o udzielenie zamówienia prowadzone jest w trybie przetargu nieograniczonego na podstawie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn.: Dz. U. z 2013 r. poz. 907 z późn. zm.), zwanej dalej „ustawą Pzp". Wartość szacunkowa zamówienia przekracza wyrażoną w złotych równowartość kwoty 134.000,00 euro.

4. ŹRÓDŁA FINANSOWANIA

Zamówienie jest finansowane ze środków budżetowych oraz częściowo ze środków Pomocy Technicznej Programu Operacyjnego Infrastruktura i Środowisko (PT POIiŚ) będących w dyspozycji Generalnego Dyrektora Dróg Krajowych i Autostrad.

5. OPIS PRZEDMIOTU ZAMÓWIENIA

5.1 Przedmiotem zamówienia jest dostawa dla GDDKIA nowych licencji, aktualizacja już użytkowanych licencji oraz wsparcie techniczne i opieka serwisowa przez okres 36 miesięcy od daty podpisania umowy.
Oznaczenie przedmiotu zamówienia wg CPV: 48223000-7 (pakiety oprogramowania dla poczty elektronicznej), 48620000-0 (systemy operacyjne), 48760000-3 (pakiety oprogramowania dla ochrony antywirusowej).

5.2. Zamawiający nie dopuszcza składania ofert częściowych.

5.3. Zamawiający nie przewiduje udzielanie zamówień uzupełniających, o których mowa w art. 67 ust. 1 pkt 7 ustawy Pzp.

5.4. Zamawiający nie dopuszcza składania ofert wariantowych.

5.5. Wykonawca ma obowiązek wskazania w ofercie (Formularz Oferty, pkt. 7) części zamówienia, którą zamierza powierzyć podwykonawcom – brak ww. informacji oznaczać będzie, iż całość zamówienia będzie realizowana przez Wykonawcę.

6. TERMIN WYKONANIA ZAMÓWIENIA

Wykonawca nie później niż w czasie 14 dni po podpisaniu umowy dostarczy Zamawiającemu do Centrali GDDKiA nośniki z wersją instalacyjną oraz klucze aktywacyjne, a także dokumenty niezbędne do uruchomienia dostępu do oprogramowania i uprawniające do korzystania z licencji. Usługi w zakresie wsparcia technicznego i opieki serwisowej producenta oprogramowania będą świadczone przez okres 36 miesięcy od dnia zawarcia umowy.

7. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW

7.1. W postępowaniu mogą brać udział Wykonawcy niepodlegający wykluczeniu z powodu niespełnienia warunków, o których mowa w art. 24 ust. 1 ustawy Pzp oraz spełniający warunki, o których mowa w art. 22 ust. 1 ustawy Pzp i określone w pkt 7.2.

7.2. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają warunki dotyczące:

1) posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania:
Zamawiający odstępuje od opisu sposobu dokonywania oceny spełniania warunków w tym zakresie. Zamawiający dokona oceny spełnienia warunków udziału w postępowaniu w tym zakresie na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu złożonego zgodnie z treścią Załącznika nr 1 do formularza „Oferta".

2) posiadania wiedzy i doświadczenia:
Zamawiający odstępuje od opisu sposobu dokonywania oceny spełniania warunków w tym zakresie. Zamawiający dokona oceny spełnienia warunków udziału w postępowaniu w tym zakresie na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu złożonego zgodnie z treścią Załącznika nr 1 do formularza „Oferta".

3) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia:

a) Potencjał techniczny
Zamawiający odstępuje od opisu sposobu dokonywania oceny spełniania warunków w tym zakresie. Zamawiający dokona oceny spełnienia warunków udziału w postępowaniu w tym zakresie na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu złożonego zgodnie z treścią Załącznika nr 1 do formularza „Oferta".

b) Potencjał kadrowy
Zamawiający odstępuje od opisu sposobu dokonywania oceny spełniania warunków w tym zakresie. Zamawiający dokona oceny spełnienia warunków udziału w postępowaniu w tym zakresie na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu złożonego zgodnie z treścią Załącznika nr 1 do formularza „Oferta".

4) sytuacji ekonomicznej i finansowej:
Zamawiający odstępuje od opisu sposobu dokonywania oceny spełniania warunków w tym zakresie. Zamawiający dokona oceny spełnienia warunków udziału w postępowaniu w tym zakresie na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu złożonego zgodnie z treścią Załącznika nr 1 do formularza „Oferta".

7.3. Wykonawca może polegać na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonywania zamówienia lub zdolnościach finansowych innych podmiotów niezależnie od charakteru prawnego łączącego go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest **udowodnić Zamawiającemu**, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia.
Zamawiający w celu oceny, czy wykonawca będzie dysponował zasobami innych podmiotów w stopniu niezbędnym dla należytego wykonania zamówienia oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, żąda dokumentów (wystawionych i podpisanych przez podmiot trzeci) dotyczących w szczególności:

- zakresu dostępnych Wykonawcy zasobów innego podmiotu,
- sposobu wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia,

- charakteru stosunku, jaki będzie łączył Wykonawcę z innym podmiotem,
- zakresu i okresu udziału innego podmiotu przy wykonywaniu zamówienia.

7.4. W przypadku wykonawców ubiegających się wspólnie o udzielenie zamówienia, żaden z nich nie może podlegać wykluczeniu z powodu niespełnienia warunków, o których mowa w art. 24 ust. 1 ustawy Pzp, natomiast spełnienie warunków wskazanych w art. 22 ust. 1 ustawy Pzp, których opis sposobu dokonywania oceny ich spełniania został zamieszczony w pkt. 7.2. SIWZ, Wykonawcy wykazują łącznie.

8. DOKUMENTY WYMAGANE W CELU WYKAZANIA BRAKU PODSTAW DO WYKLUCZENIA Z POSTĘPOWANIA ORAZ POTWIERDZENIA SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ NA POTWIERDZENIE, ŻE OFEROWANE DOSTAWY I USŁUGI ODPOWIADAJĄ WYMAGANIOM ZAMAWIAJĄCEGO

8.1. W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia, potwierdzenia spełnienia warunków udziału w postępowaniu oraz wykazania, że oferowane dostawy i usługi spełniają wymagania Zamawiającego, wykonawcy muszą złożyć wraz z ofertą następujące oświadczenia i dokumenty:

8.1.1. Oświadczenie o spełnianiu warunków określonych w art. 22 ust. 1 ustawy Pzp zgodne z treścią Załącznika nr 1 do formularza „Oferta" oraz oświadczenie o braku podstaw do wykluczenia z postępowania z powodu niespełnienia warunków określonych w art. 24 ust. 1 ustawy Pzp, zgodne z treścią Załącznika nr 2 do formularza „Oferta". Oświadczenie o spełnieniu warunków określonych w art. 22 ust. 1 ustawy Pzp powinno być złożone w imieniu wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia. Oświadczenie o braku podstaw do wykluczenia z postępowania z powodu niespełnienia warunków określonych w art. 24 ust. 1 ustawy Pzp powinno być złożone przez każdego z Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

8.1.2. Aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

8.1.3. Aktualne zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzające, że Wykonawca nie zalega z opłacaniem podatków lub zaświadczenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

8.1.4. Aktualne zaświadczenie właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzające, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenie zdrowotne i społeczne, lub potwierdzenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

8.1.5. Aktualną informację z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 4-8 i 10-11 ustawy, wystawioną nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

8.1.6. Aktualną informację z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9 ustawy, wystawioną nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

8.1.7. Listę podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy Pzp, albo informację o tym, że Wykonawca nie należy do grupy kapitałowej (zgodnie z treścią Załącznika nr 3 do formularza „Oferta").

8.1.8. W przypadku zaproponowania oprogramowania firmy Microsoft, na potwierdzenie, że oferowane usługi i dostawy odpowiadają wymaganiom Zamawiającego, należy do oferty załączyć dokument potwierdzający, że Wykonawca posiada aktualny status Large Account Reseller (LAR) firmy Microsoft i jest upoważniony do przedłużenia umowy Microsoft Enterprise Nr E2598560 z dnia 29.07.2011 r., zawartej przez Zamawiającego z Microsoft Ireland Operations Limited B.V., a następnie do dalszej obsługi tej umowy.
Powyższe wymaganie nie dotyczy ofert złożonych przez Wykonawców oferujących rozwiązania równoważne.

8.1.9. Na potwierdzenie, że oferowane usługi i dostawy odpowiadają wymaganiom Zamawiającego, do oferty należy załączyć wykaz oferowanych produktów wraz z podaniem w szczególności nazwy oprogramowania, jego identyfikatora stosowanego przez producenta, liczby licencji i ceny jednostkowej za cały okres trwania umowy wraz z podatkiem VAT.

UWAGA: W przypadku zaoferowania produktów równoważnych (innych niż producenta Microsoft), z uwagi na to, że art. 30 ust. 5 ustawy prawo zamówień publicznych wyraźnie wskazuje na Wykonawcę jako tego, który jest zobowiązany wykazać, że oferowane rozwiązania i produkty spełniają wymagania postawione przez Zamawiającego, Zamawiający zastrzega sobie prawo sprawdzenie pełnej zgodności oferowanych produktów z wymogami specyfikacji. Sprawdzenie to, będzie polegać na wielokrotnym przeprowadzeniu testów w warunkach produkcyjnych na sprzęcie Zamawiającego, z użyciem urządzeń peryferyjnych Zamawiającego, na arkuszach, bazach danych i plikach Zamawiającego. W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby zamawiającego w terminie 5 dni od daty otrzymania wezwania, po jednym egzemplarzu wskazanego przedmiotu zamówienia. W odniesieniu do oprogramowania 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. Negatywny wynik tego sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 89 ust. 1 pkt. 2 ustawy. Nie przedłożenie oferowanych produktów do przetestowania w ww. terminie zostanie potraktowane, jako negatywny wynik sprawdzenia. Po wykonaniu testów, dostarczone do testów egzemplarze będą zwrócone wykonawcy.

8.2. Dokumenty, o których mowa w pkt 8, sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

8.3. Dokumenty, o których mowa w pkt. 8 (za wyjątkiem oświadczenia o spełnianiu warunków określonych w art. 22 ust. 1 ustawy Pzp, które musi zostać złożone w formie oryginału) powinny być złożone w oryginale lub kopii poświadczonej za zgodność z oryginałem przez Wykonawcę.

8.4. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia oraz w przypadku podmiotów, o których mowa w pkt 7.3, kopie dokumentów dotyczących odpowiednio Wykonawcy lub tych podmiotów są poświadczane za zgodność z oryginałem przez Wykonawcę lub te podmioty.
Poświadczenie za zgodność z oryginałem powinno być sporządzone w sposób umożliwiający identyfikację podpisu (np. wraz z imienną pieczątką osoby poświadczającej kopię dokumentu za zgodność z oryginałem).
Zamawiający zażąda przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentu wyłącznie wtedy, gdy złożona kopia dokumentu będzie nieczytelna lub będzie budziła wątpliwości co do jej prawdziwości.

8.5. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w pkt 8.1.

1) 8.1.2 – 8.1.4 i 8.1.6 - składa dokument lub dokumenty, wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
   a) nie otwarto jego likwidacji ani nie ogłoszono upadłości,

b) nie zalega z uiszczaniem podatków, opłat, składek na ubezpieczenie społeczne i zdrowotne albo że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
c) nie orzeczono wobec niego zakazu ubiegania się o zamówienia;

2) 8.1.5 – składa zaświadczenie właściwego organu sądowego lub administracyjnego miejsca zamieszkania albo zamieszkania osoby, której dokumenty dotyczą, w zakresie określonym w art. 24 ust. 1 pkt. 4-8 ustawy Pzp.

8.6. Dokumenty, o których mowa w pkt. 8.5. 1) lit. a) i c) oraz w pkt. 2) powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert. Dokument, o którym mowa w pkt. 8.5. 1) lit. b) powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

8.7. Jeżeli w miejscu zamieszkania osoby lub w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt. 8.5., zastępuje się je dokumentem zawierającym oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio miejsca zamieszkania osoby lub kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania. Przepis pkt. 8.6. stosuje się odpowiednio.

8.8. Każdy z Wykonawców składających wspólną ofertę musi złożyć dokumenty wymienione w pkt 8.1.2. – 8.1.7 albo odpowiadające im określone w pkt 8.5., 8.7. lub 8.9. Dokumenty wymienione w pkt. 8.1.8 i 8.1.9 winny być przedłożone w imieniu wszystkich Wykonawców składający wspólną ofertę.

8.9. Jeżeli, w przypadku Wykonawcy mającego siedzibę na terytorium Rzeczypospolitej Polskiej, osoby, o których mowa w art. 24 ust. 1 pkt 5—8, 10 i 11 ustawy Pzp, mają miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, Wykonawca składa w odniesieniu do nich zaświadczenie właściwego organu sądowego albo administracyjnego miejsca zamieszkania dotyczące niekaralności tych osób w zakresie określonym w art. 24 ust.1 pkt 5—8, 10 i 11 ustawy Pzp, wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert, z tym, że w przypadku, gdy w miejscu zamieszkania tych osób nie wydaje się takich zaświadczeń — zastępuje się je dokumentem zawierającym oświadczenie złożone przed właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego miejsca zamieszkania tych osób lub przed notariuszem.

8.10. W przypadku, o którym mowa w pkt. 7.3. SIWZ Wykonawca wraz z ofertą składa dokumenty wskazane w tym punkcie.

9. OPIS SPOSOBU PRZYGOTOWANIA OFERT

9.1. Wykonawca może złożyć jedną ofertę.

9.2. Oferta winna zawierać wypełniony i podpisany formularz „Oferta" oraz wszelkie Załączniki wymagane postanowieniami niniejszej SIWZ, w tym:

9.3. Do oferty należy załączyć:

9.3.1. Dokumenty wymagane postanowieniami pkt 8 niniejszej SIWZ.

9.3.2. Pełnomocnictwo do podpisania oferty oraz do podpisania innych dokumentów i oświadczeń składanych wraz z ofertą, o ile prawo do ich podpisania nie wynika z innych dokumentów złożonych wraz z ofertą. Treść pełnomocnictwa musi jednoznacznie wskazywać czynności, do wykonywania, których pełnomocnik jest upoważniony. Pełnomocnictwo winno być złożone w oryginale lub kopii poświadczonej za zgodność z oryginałem przez notariusza.

9.3.3. W przypadku Wykonawców wspólnie ubiegających się o zamówienia, pełnomocnictwo do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia. Pełnomocnictwo lub pełnomocnictwa winny być złożone w oryginale lub kopii poświadczonej za zgodność z oryginałem przez notariusza.

9.3.4. Dowód wniesienia wadium. W przypadku, gdy wadium wnoszone jest w innej formie niż pieniądz, Wykonawca winien złożyć oryginał gwarancji lub poręczenia.

9.4. Oferta wraz z załącznikami powinna być zgodna, zarówno w sposobie jej sporządzenia, jak i zawartości merytorycznej ze wszystkimi wymaganiami określonymi w niniejszej Specyfikacji Istotnych Warunków Zamówienia. Oferta oraz pozostałe oświadczenia i dokumenty, dla których Zamawiający określił wzory w formie formularzy zamieszczonych w Rozdziale IV, winny być sporządzone zgodnie z tymi wzorami, co do treści oraz opisu kolumn i wierszy. Zamawiający dopuszcza modyfikację wzorów, w sposób nienaruszający wymagań niniejszej SIWZ. Każdy dokument składający się na ofertę musi być czytelny. Oferta wraz z załącznikami powinna być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy.

9.5. Oferta musi być sporządzona w języku polskim. Dokumenty sporządzone w innym języku winny być złożone wraz z tłumaczeniem na język polski.

9.6. Każde oświadczenie składające się na ofertę musi być podpisane w sposób wiążący Wykonawcę lub Wykonawców (w przypadku wspólnego ubiegania się o zamówienie). Każda poprawka w treści oferty, a w szczególności każde przerobienie, przekreślenie, uzupełnienie, nadpisanie, przesłonięcie korektorem, etc. muszą być parafowane przez Wykonawcę.

9.7. Każda zawierająca jakąkolwiek treść strona oferty powinna być ponumerowana i podpisana lub parafowana przez Wykonawcę. Strony oferty powinny być trwale ze sobą połączone i kolejno ponumerowane.

9.8. Zamawiający informuje, iż zgodnie z art. 8 ust. 3 ustawy Prawo zamówień publicznych, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy Pzp. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.), które Wykonawca pragnie zastrzec przed dostępem dla innych uczestników postępowania, winny być załączone na końcu oferty w osobnym opakowaniu, w sposób umożliwiający łatwe od niej odłączenie i opatrzone napisem: *„Informacje stanowiące tajemnicę przedsiębiorstwa – nie udostępniać innym uczestnikom postępowania*", z zachowaniem kolejności numerowania stron oferty.

9.9. Ofertę należy sporządzić w 1 egzemplarzu i umieścić w zamkniętym opakowaniu, uniemożliwiającym odczytanie jej zawartości bez uszkodzenia tego opakowania. Opakowanie winno być oznaczone nazwą (firmą) i adresem Wykonawcy, zaadresowane do Zamawiającego na adres:

Generalna Dyrekcja Dróg Krajowych i Autostrad
ul. Wronia 53
00-874 Warszawa

oraz opisane:

„DOSTAWA DLA GDDKiA NOWYCH LICENCJI, AKTUALIZACJA JUŻ UŻYTKOWANYCH LICENCJI ORAZ WSPARCIE TECHNICZNE I OPIEKA SERWISOWA"

„Nie otwierać przed dniem 13 maja 2014 r. godz. 11.15"

9.10. Wszelkie konsekwencje mogące wynikać z niezachowania powyższych wymagań będą obciążały Wykonawcę.

9.11. Przed upływem terminu składania ofert, Wykonawca może wprowadzić zmiany do złożonej oferty lub wycofać ofertę. Oświadczenia o wprowadzonych zmianach lub wycofaniu oferty powinny być doręczone Zamawiającemu na piśmie pod rygorem nieważności przed upływem terminu składania ofert. Oświadczenia powinny być opakowane tak, jak oferta, a opakowanie powinno zawierać odpowiednio dodatkowe oznaczenie wyrazem: „ZMIANA" lub „WYCOFANIE".

10. OPIS SPOSOBU OBLICZENIA CENY

10.1 Cena oferty zostanie przedstawiona przez Wykonawcę w Formularzu „Oferta".

10.2. Cena za realizację przedmiotu zamówienia musi być skalkulowana w sposób jednoznaczny, uwzględniać wszystkie wymagania Zamawiającego określone w SIWZ oraz obejmować wszelkie koszty związane z realizacją przedmiotu zamówienia.

10.3. Walutą ceny oferowanej jest złoty polski (PLN).

10.4. Cena ofertowa powinna być podane z dokładnością do 1 grosza, tj. do dwóch miejsc po przecinku.

10.5. Wszelkie rozliczenia dotyczące realizacji przedmiotu zamówienia opisanego w niniejszej specyfikacji dokonywane będą w złotych polskich.

10.6. Cena określona przez Wykonawcę zostanie podana jako wartość brutto oferty złożonej przez Wykonawcę, tj. wraz z należnym podatkiem VAT od towarów i usług, w wysokości przewidzianej ustawowo.

11. OPIS SPOSOBU UDZIELANIA WYJAŚNIEŃ TREŚCI SIWZ

11.1. Wykonawca może zwrócić się do Zamawiającego z prośbą o wyjaśnienie treści SIWZ, a Zamawiający odpowie niezwłocznie na pytanie, jednak nie później niż na 6 dni przed upływem terminu składania ofert – pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SIWZ.

11.2. Zamawiający nie przewiduje zebrania Wykonawców.

11.3. Formą porozumiewania się w trakcie postępowania o udzielenie zamówienia oraz postępowania odwoławczego jest forma pisemna lub faksem. Zamawiający wymaga niezwłocznego potwierdzenia przez Wykonawcę pisemnie lub faksem faktu otrzymania każdej informacji przekazanej faksem, a na żądanie Wykonawcy potwierdzi fakt otrzymania od niego informacji. Oświadczenia, wnioski, zawiadomienia, oraz informacje przekazane za pomocą faksu uważa się za złożone w terminie, jeżeli ich treść jest czytelna dotarła do Zamawiającego przed upływem wyznaczonego terminu.

Osoby do kontaktu oraz nr faksu Zamawiającego:

- w sprawach przedmiotu zamówienia: Dariusz Nowak (022) 375 86 44,
- w sprawach procedury: Anita Zakościelna tel.: (022) 375 86 67, faks: (022) 375 86 21.

Wszelkie informacje dotyczące niniejszego postępowania (przewidziane ustawą Pzp) będą udostępniane na stronie internetowej www.gddkia.gov.pl

12. TERMIN ZWIĄZANIA OFERTĄ

Termin związania ofertą wynosi 60 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

13. MIEJSCE I TERMIN SKŁADANIA I OTWARCIA OFERT

13.1. Oferty winny być złożone w siedzibie Zamawiającego **w Warszawie ul. Wronia 53, w Kancelarii, I piętro, pokój nr 163 w terminie do dnia 13 maja 2014 roku, do godziny 11.00.**

13.2. Otwarcie ofert odbędzie się w siedzibie Zamawiającego w dniu, w którym upływa termin składania ofert, o godzinie 11.15.

13.3 Otwarcie ofert jest jawne.

14. WYMAGANIA DOTYCZĄCE WADIUM

14.1. Oferta powinna być zabezpieczona wadium w wysokości: 250.000,00 PLN (słownie: dwieście pięćdziesiąt tysięcy złotych).

14.2. Wadium musi być wniesione przed upływem terminu składania ofert w formie określonej w art. 45 ust. 6 ustawy Pzp.

14.3. Wadium wnoszone w pieniądzu winno być wpłacone na rachunek bankowy BGK 95 1130 1017 0020 1172 7820 0010.

14.4. Zamawiający dokona zwrotu wadium na zasadach określonych w art. 46 ust. 1-4 ustawy Pzp.
14.5. Wykonawca utraci wadium w przypadkach określonych w art. 46 ust. 4a oraz ust. 5 ustawy Pzp.
14.6. Wadium musi obejmować cały okres związania ofertą.
14.7. Zamawiający zażąda ponownego wniesienia wadium przez Wykonawcę, któremu zwrócono wadium na podstawie art. 46 ust. 1, jeżeli w wyniku rozstrzygnięcia odwołania jego oferta zostanie wybrana jako najkorzystniejsza. Wykonawca wnosi wadium w terminie określonym przez Zamawiającego.

15. KRYTERIA WYBORU OFERTY NAJKORZYSTNIEJSZEJ

15.1. Przy dokonywaniu wyboru najkorzystniejszej oferty Zamawiający stosować będzie wyłącznie kryterium ceny.
15.2. Ocena kryterium będzie dokonywana według wzoru:

$$W = \frac{\text{najniższa cena w ofertach}}{\text{cena w ofercie badanej}} \times 100 \text{ pkt}$$

W – wartość oceny oferty według kryterium

15.3. Oferta nie odrzucona, zawierająca najniższą cenę zostanie uznana za ofertę najkorzystniejszą.

16. UDZIELENIE ZAMÓWIENIA

16.1 Zamawiający udzieli zamówienia temu Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą.
16.2. W przypadku Wykonawców, którzy wspólnie ubiegają się o udzielenie zamówienia a ich oferta zostanie uznana za najkorzystniejszą, zobowiązany będzie po uprawomocnieniu się decyzji o wyborze jego oferty, a przed podpisaniem umowy przedłożyć do wglądu Zamawiającemu umowę konsorcjum stwierdzającą solidarną odpowiedzialność wszystkich Wykonawców za realizację zamówienia oraz zawierającą upoważnienie dla jednego z Wykonawców do składania i przyjmowania oświadczeń wobec Zamawiającego w imieniu wszystkich Wykonawców, a także do otrzymywania należnych płatności.
16.3. O terminie na przedłożenie powyższych dokumentów Wykonawca zostanie powiadomiony przez Zamawiającego odrębnym pismem.

17. INFORMACJA O NALEŻYTYM ZABEZPIECZENIU WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

18. INFORMACJE O FORMALNOŚCIACH, JAKICH NALEŻY DOPEŁNIĆ PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY

Wykonawca przed zawarciem umowy na wezwanie Zamawiającego poda wszelkie informacje niezbędne do wypełnienia treści umowy.

19. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ

19.1. Wykonawcy, a także innemu podmiotowi, który ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów Ustawy Pzp, przysługują środki ochrony prawnej przewidziane w art. 179 i następnych ustawy Pzp.
19.2. Wobec niezgodnej z przepisami ustawy Pzp czynności Zamawiającego podjętej w toku postępowania lub w przypadku zaniechania przez Zamawiającego dokonania czynności, do których podjęcia zobowiązany jest Zamawiający przepisami ustawy Pzp, Wykonawca może wnieść odwołanie.
19.3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo elektronicznej opatrzonej bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu.

19.4. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, a by mógł on zapoznać się z jego treścią przed upływem tego terminu.

19.5. Odwołanie wnosi się w terminie 10 dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli informacje te zostały przesłane faksem lub drogą elektroniczną, albo w terminie 15 dni - jeżeli informacje zostały przesłane w inny sposób.

19.6. Odwołanie wobec treści ogłoszenia o zamówieniu oraz specyfikacji istotnych warunków zamówienia wnosi się w terminie 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia specyfikacji istotnych warunków zamówienia na stronie internetowej.

19.7. Odwołanie wobec czynności innych niż wymienione w pkt 19.5 i 19.6 wnosi się w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

ROZDZIAŁ II
SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa dla GDDKIA nowych licencji, aktualizacja już posiadanych licencji oraz wsparcie techniczne i opieka serwisowa producenta oprogramowania przez okres 36 miesięcy od daty zawarcia umowy.

Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych.

W przypadku zaoferowania przez Wykonawcę rozwiązań równoważnych (innych niż użytkowane i wykorzystywane w GDDKiA), Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia przez Zamawiającego oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), poziomu serwisu gwarancyjnego (nie gorszego niż obecnie posiadany) oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania (sprzęt, oprogramowanie).

Specyfikacja ilościowa przedmiotu zamówienia (Produktów):

Typ oprogramowania	Liczba licencji
Prawo do uaktualniania posiadanych Systemów Operacyjnych Desktop PC	5343
Prawo do uaktualnienia posiadanego pakietu biurowego	5258
Prawo do uaktualniania posiadanego pakietu licencji dostępowych (licencje na urządzenie)	5258
Pakiet Biurowy z prawem do uaktualniania	85
Pakiet Licencji Dostępowych z prawem do uaktualniania (licencje na urządzenie)	85
Pakiet usług hostowanych wraz subskrypcją Pakietu Biurowego	5343
Prawo do uaktualniania serwera poczty elektronicznej typ I (licencja na serwer)	4
Prawo do uaktualniania serwera poczty elektronicznej typ II (licencja na serwer)	2
System zarządzania środowiskami serwerowymi bez serwerowego systemu operacyjnego (licencja na 2 procesory)	164
Serwerowy system operacyjny z elementami zarządzania z prawem do uaktualnienia (licencja na 2 procesory)	10
Serwer portalu internet i intranet z prawem do uaktualnienia (licencja na serwer)	1
Serwer komunikacji wielokanałowej z prawem do uaktualnienia (licencja na serwer)	1
Prawo do uaktualniania serwera bazy danych (licencja na 2 rdzenie procesora)	6
Prawo do uaktualniania pakietu zarządzania projektami	28
Pakiet zarządzania projektami z prawem do uaktualniania	21
Prawo do uaktualniania pakietu modelowania graficznego	21
Pakiet modelowania graficznego z prawem do uaktualniania	3
Platforma usług hostowanych	1 pakiet
Pakiet usług standardowych opieki serwisowej do oprogramowania będącego przedmiotem dostawy	2 pakiety

Tabela 1 – specyfikacja ilościowa zamawianych Produktów

1. Wymagania ogólne

W przypadku zaoferowania rozwiązań równoważnych wraz z ofertą Wykonawca złoży dokument opisujący zasady licencjonowania udzielane standardowo do oferowanego oprogramowania oraz zasady świadczenia usług standardowych opieki serwisowej do oprogramowania, nie gorsze od wymogów zawartych w SIWZ.

Wymagania ogólne w zakresie dostaw:

1. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi i serwerami (np. w przypadku wymiany sprzętu).
2. Licencje muszą upoważniać Zamawiającego do korzystania z oprogramowania co najmniej w zakresie określonym w umowie, w tym w pkt. 2 – 2.19.
3. Prawo do uaktualniania oznacza prawo do instalacji najnowszej wersji oprogramowania dostępnej w okresie minimum 35 miesięcy.
4. Licencjonowanie musi uwzględniać prawo (w okresie przynajmniej 5 lat od dnia zawarcia umowy) do instalacji udostępnianych przez producenta oprogramowania uaktualnień i poprawek krytycznych i opcjonalnych do zakupionych wersji oprogramowania.
5. Z uwagi na zakres funkcjonalny wdrożenia planowanego na bazie zamawianego oprogramowania, konieczności wprowadzenia jednolitych polityk bezpieczeństwa oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga oferty zawierającej licencje pochodzące od jednego producenta, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania i monitorowania.
6. Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania i korzystania z kopii zamiennych (możliwość kopiowanie oprogramowania na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych.
7. Wykonawca zapewni dostęp do spersonalizowanej strony producenta oprogramowania pozwalającej upoważnionym osobom ze strony Zamawiającego na:
   a) Pobieranie zakupionego oprogramowania,
   b) Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania,
   c) Sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów.
8. Zamawiający wymaga dostępu do oprogramowania i kluczy licencyjnych w terminie do 14 dni od zawarcia umowy.
9. Po dziewięćdziesięciu (90) dniach od zakończenia okresu trwania umowy i wypadku nie podjęcia decyzji o jej przedłużeniu Wykonawca zapewni wyłączenie konta na spersonalizowanej stronie dedykowanej Zamawiającemu i usunięcie jego danych.
10. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu osoby trzeciej przypadku, gdyby osoby trzecie zgłosiły uzasadnione roszczenia wobec Zamawiającego wynikające z tytułu naruszeń praw, określonych w umowie, Wykonawca zobowiązuje się do zaspokojenia roszczeń skierowanych do Zamawiającego z tych tytułów wraz z kosztami postępowania sądowego i zastępstwa procesowego. W przypadku pozwania Zamawiającego z tytułu naruszenia praw osób trzecich, Wykonawca wstąpi do postępowania sądowego w

charakterze pozwanego, a w razie braku takiej możliwości wystąpi z interwencją uboczną po stronie Zamawiającego.

11. 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.

12. W ramach wykonania umowy i dostaw produktów opisanych w specyfikacji Zamawiający ma mieć prawo do testowania oprogramowania i korzystania z oprogramowania w celach edukacyjnych wszystkich produktów producenta oprogramowania bez dodatkowych opłat. Wówczas Zamawiający nabywa prawo do uruchamiania:

    - 20 kopii każdego produktu w celach edukacyjnych (w wydzielonym pomieszczeniu, przeznaczonym do szkoleń) bez konieczności dostaw dodatkowych licencji,

    - 10 kopii każdego produktu w celach testowych w 60-dniowym okresie ewaluacyjnym, po którym istnieje możliwość zamówienia odpowiedniej ilość licencji na testowany produkt.

13. Wykonawca zapewni w trakcie jej trwania, tj. w okresie 36 miesięcy, możliwość używania pakietu biurowego określonego w pkt. 2.2. na domowych komputerach pracowników Zamawiającego bez dodatkowej opłaty za licencję.

2. Specyfikacja techniczno – eksploatacyjna i cech użytkowych oprogramowania.

Poniżej przedstawione są wymagania funkcjonalne dotyczące zamawianego oprogramowania i usług.
Z uwagi na to, że art. 30 ust. 5 ustawy prawo zamówień publicznych wyraźnie wskazuje na Wykonawcę, jako tego, kto jest zobowiązany wykazać, że oferowane rozwiązania i produkty spełniają wymagania postawione przez Zamawiającego, Zamawiający zastrzega sobie, w przypadku jakichkolwiek wątpliwości, prawo sprawdzenie pełnej zgodności oferowanych produktów z wymogami specyfikacji. Sprawdzenie to, będzie polegać na wielokrotnym przeprowadzeniu testów w warunkach produkcyjnych na sprzęcie Zamawiającego, z użyciem urządzeń peryferyjnych Zamawiającego, na arkuszach, bazach danych i plikach Zamawiającego.
W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, po jednym egzemplarzu wskazanego przedmiotu dostawy. W odniesieniu do oprogramowania 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. Negatywny wynik tego sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 89 ust. 1 pkt. 2 ustawy.
Nie przedłożenie oferowanych produktów do przetestowania w ww. terminie zostanie potraktowane, jako negatywny wynik sprawdzenia.
Po wykonaniu testów, dostarczone do testów egzemplarze będą zwrócone oferentowi.

2.1. Prawo do uaktualniania posiadanych Systemów Operacyjnych Desktop PC

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

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy.
   b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.
2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim.
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.
4. Wbudowany system pomocy w języku polskim.
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.
6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne.
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
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 logowania do domeny w oparciu o:
    a. Login i hasło.
    b. Karty z certyfikatami (smartcard).
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
27. Mechanizmy wieloelementowego 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. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.
32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.
35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
36. 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.
37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
40. Udostępnianie modemu.
41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
43. 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.).
44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.
46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.
47. 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.

48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
51. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB).
52. 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.
53. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie.
54. 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.
55. 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.
56. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
57. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC.
58. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
59. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
60. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów.
61. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M.
62. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
63. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia.
64. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache".
65. 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.
66. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością.
67. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji.
68. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
69. Funkcjonalność umożliwiająca na zaktualizowanie klienta systemu bez potrzeby aktualizacji, przebudowywania paczek aplikacji.
70. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
71. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
72. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym.
73. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
74. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet.
75. Funkcjonalność migracji ustawień aplikacji pomiędzy wieloma komputerami.

2.2. Prawo do uaktualnienia posiadanego pakietu biurowego

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

1. 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.
2. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi Active Directory.
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 nr 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 wykorzystanie schematów XML.
   d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES.
5. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
6. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.

7. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
8. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
9. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a. Edytor tekstów
   b. Arkusz kalkulacyjny
   c. Narzędzie do przygotowywania i prowadzenia prezentacji
   d. Narzędzie do tworzenia i wypełniania formularzy elektronicznych
   e. Narzędzie do tworzenia drukowanych materiałów informacyjnych
   f. Narzędzie do tworzenia i pracy z lokalną bazą danych
   g. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
   h. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR
   i. 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 2003 lub Microsoft Word 2007 i 2010 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. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
    s. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

11. Arkusz kalkulacyjny musi umożliwiać:
    a. Tworzenie raportów tabelarycznych.
    b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
    c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
    d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
    e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
    f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
    g. Wyszukiwanie i zamianę danych.
    h. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
    i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
    j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
    k. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
    l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
    m. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
    n. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
    o. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
    p. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
12. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    a. Przygotowywanie prezentacji multimedialnych, które będą:
    b. Prezentowanie przy użyciu projektora multimedialnego.
    c. Drukowanie w formacie umożliwiającym robienie notatek.
    d. Zapisanie jako prezentacja tylko do odczytu.
    e. Nagrywanie narracji i dołączanie jej do prezentacji.
    f. Opatrywanie slajdów notatkami dla prezentera.
    g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
    h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
    i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
    j. Możliwość tworzenia animacji obiektów i całych slajdów.
    k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
    l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.
13. Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:
    a. Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania.

b. Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków.
c. Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników.
d. Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych.
e. Możliwość pobierania danych z platformy do pracy grupowej.
f. Przesłanie danych przy użyciu usługi Web (tzw. web service).
g. Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.
h. Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.

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. 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 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.

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. 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.
    d. Możliwość obsługi tekstowych wiadomości błyskawicznych.
    e. Możliwość komunikacji głosowej i video.
    f. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
    g. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
    h. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

2.3. Prawo do uaktualniania posiadanego pakietu licencji dostępowych (licencje na urządzenie)

Pakiet licencji dostępowych musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników funkcjonalności serwerów producenta oferowanego oprogramowania:

1. Serwerowych systemów operacyjnych.
2. Serwerów portali intranet.
3. Serwerów poczty elektronicznej.
4. Serwerów systemu zarządzania infrastrukturą i oprogramowaniem.

5. Podstawowej funkcjonalności serwerów komunikacji wielokanałowej (wskazanych w pkt. 2.6 „Usługa serwera komunikacji wielokanałowej on-line”).
6. Klienta systemu antywirusowego.

2.4. Pakiet Biurowy z prawem do uaktualniania

Licencje Pakietu Biurowego opisanego powyżej z prawem do uaktualniania.

2.5. Pakiet Licencji Dostępowych z prawem do uaktualniania (licencje na urządzenie)

Pakiet licencji dostępowych opisanych powyżej z prawem do uaktualniania.

2.6. Pakiet usług hostowanych wraz subskrypcją Pakietu Biurowego

Pakiet usług hostowanych (on-line) ma uprawniać użytkowników do wykorzystania usług on-line – portalu wewnętrznego, poczty elektronicznej oraz narzędzi wiadomości błyskawicznych i konferencji głosowych i video. Ponadto musi zawierać 36 miesięczną subskrypcję pakietu biurowego.

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 (2007 i 2010),
- Przeglądarki (Web Access),
- Urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe (do 25GB),
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa funkcji klienta poczty elektronicznej takich jak tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy,

zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla przeglądarek internetowych,

- Współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy,
- Bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

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

1. Funkcjonalność podstawowa:
   a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.
   b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.
   c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami.
   d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia.
   e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
2. Funkcjonalność wspierająca pracę grupową:
   a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości.
   b. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.
   c. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze.
   d. Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone.
   e. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania.
   f. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań.
   g. Obsługa list i grup dystrybucyjnych.
   h. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.
   i. Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu.

j. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.

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

l. 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.

m. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.

n. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.

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

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

3. Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:

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

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

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

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

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

f. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.

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

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

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

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

4. Wsparcie dla użytkowników mobilnych:

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

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

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

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

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

Obsługa interfejsu dostępu do poczty w przeglądarkach internetowych.

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. Umożliwienie stosowania narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML.
    c. Umożliwienie stosowania technologii 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. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.

g. 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:

a. Wymagania odnośnie interfejsu użytkownika:

b. Pełna polska wersja językowa interfejsu użytkownika.

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

d. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:

   i. posiada kompletny i publicznie dostępny opis formatu.

   ii. ma zdefiniowany układ informacji w postaci XML umożliwiający wykorzystanie schematów XML, wspierający podpis elektroniczny.

e. Pakiet biurowy on-line musi zawierać:

   i. Edytor tekstów.

   ii. Arkusz kalkulacyjny.

   iii. Narzędzie do przygotowywania i prowadzenia prezentacji.

   iv. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.

f. Edytor tekstów musi umożliwiać:

   i. 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.

   ii. Wstawianie oraz formatowanie tabel.

   iii. Wstawianie oraz formatowanie obiektów graficznych.

   iv. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).

   v. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.

   vi. Automatyczne tworzenie spisów treści.

   vii. Formatowanie nagłówków i stopek stron.

   viii. Sprawdzanie pisowni w języku polskim.

   ix. Śledzenie zmian wprowadzonych przez użytkowników.

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

xi. Określenie układu strony (pionowa/pozioma).

xii. Wydruk dokumentów.

xiii. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.

xiv. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.

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

xvi. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.

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

g. Arkusz kalkulacyjny musi umożliwiać:

i. Tworzenie raportów tabelarycznych.

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

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

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

v. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.

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

vii. Wyszukiwanie i zamianę danych.

viii. Wykonywanie analiz danych przy użyciu formatowania warunkowego.

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

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

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

xii. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.

xiii. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.

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

h. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

i. Przygotowywanie prezentacji multimedialnych

ii. Prezentowanie przy użyciu projektora multimedialnego.

iii. Drukowanie w formacie umożliwiającym robienie notatek.

iv. Zapisanie jako prezentacja tylko do odczytu.

v. Nagrywanie narracji i dołączanie jej do prezentacji.

vi. Opatrywanie slajdów notatkami dla prezentera.

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

viii. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.

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

x. Możliwość tworzenia animacji obiektów i całych slajdów.

xi. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.

xii. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

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

1. Prostą, efektywną kosztowo, niezawodną i bezpieczną komunikację głosową oraz video.
2. Przesyłanie wiadomości tekstowych z komputerów klasy PC wyposażonych w klienta SKW lub przeglądarkę oraz urządzeń mobilnych.
3. Możliwość organizowania telekonferencji.
4. Łączności głosowej i video z wieloma (więcej niż dwoma) uczestnikami konferencji.
5. Zarządzania połączeniami telefonicznymi i głosowymi.
6. Współdzielenia aplikacji.

Wymagana jest funkcjonalność polegająca na umożliwieniu współpracy wykorzystującej integrację poczty e-mail, kalendarzy, wiadomości błyskawicznych, konferencji w sieci Web, audio i wideokonferencji. Serwer SKW ma zapewniać natywną integrację z komponentami portalu wielofunkcyjnego i poczty elektronicznej. Ponadto SKW będzie wykorzystywała mechanizm pojedynczego logowania (single sign-on), uprawnień użytkowników i ich grup,

bazując na komponencie posiadanych usług katalogowych (Active Directory). Wynikiem takiej integracji mają być następujące cechy systemu:

7. Ujednolicenie komunikacji biznesowej:
    a. Dostęp z dowolnego miejsca do komunikacji w czasie rzeczywistym i asynchronicznej.
    b. Możliwość ujednolicenia i współdziałania poczty głosowej, e-mail, kontaktów, kalendarzy, wiadomości błyskawicznych (IM) i danych o obecności.
    c. Dostępność aplikacji klienckiej udostepniającej komunikację głosową, video i tekstową, organizowanie konferencji planowanych i ad-hoc.
    d. Dostępność aplikacji klienckiej dla uczestników telekonferencji nieposiadających licencji dostępowej do serwerów SKW z funkcjonalnością:
        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.
        vii. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji.
    e. Integracja z aplikacjami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
    f. Wbudowane mechanizmy dostępu mobilnego i bezprzewodowego.
    g. Rozszerzalna platforma integracji narzędzi współpracy z pakietem biurowym.
    h. Funkcje statusu obecności, IM i konferencji (głosowych i video) bezpośrednio wbudowane w portale i obszary robocze zespołów i dostępne z poziomu klienta poczty elektronicznej.
    i. Możliwość wspólnej pracy zespołów z różnych lokalizacji, wewnątrz i spoza ram organizacyjnych, także z wykorzystaniem przez użytkowników zewnętrznych bezpłatnych aplikacji klienckich.
8. W związku z tak postawionymi założeniami SKW ma zapewnić:
    a. Efektywną wymianę informacji z możliwością wyboru formy i kanału komunikacji i niezależnie od lokalizacji pracowników.
    b. Wykorzystanie statusu obecności i konferencje w czasie rzeczywistym.
    c. Zarządzanie, sortowanie i pracę z różnymi typami wiadomości, bez konieczności przełączania się pomiędzy aplikacjami czy systemami.
    d. Dostęp z dowolnego miejsca poprzez dostęp do usług komunikacyjnych z poziomu pulpitu, przeglądarki sieci Web i urządzeń mobilnych.
9. SKW ma zapewnić obsługę następujących funkcjonalności:

a. Status obecności – informacja o statusie dostępności użytkowników (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej, zintegrowana z usługą katalogową i kalendarzem, a dostępna w interfejsach poczty elektronicznej, komunikatora i portalu wielofunkcyjnego. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności.

b. Krótkie wiadomości tekstowe – Możliwość komunikacji typu chat. Możliwość grupowania kontaktów, możliwość konwersacji typu jeden-do-jednego, jeden-do-wielu, możliwość rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat. Możliwość komunikacji z darmowymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu. Możliwość administracyjnego zarządzania treściami przesyłanymi w formie komunikatów tekstowych.

c. Obsługa komunikacji głosowej – Możliwość realizowania połączeń głosowych między użytkownikami lokalnymi.

d. Obsługa komunikacji wideo – Możliwość zestawiania połączeń wideo-telefonicznych.

e. Obsługa konferencji wirtualnych – Możliwość realizacji konferencji wirtualnych z wykorzystaniem głosu i wideo. Możliwość współdzielenia aplikacji jak również całego pulpitu.

f. Możliwość nagrywania konferencji na centralnym serwerze jak również lokalnie przez uczestników.

g. Automatyzacja planowania konferencji - zaproszenia rozsyłane są automatycznie w postaci poczty elektronicznej.

h. Wsparcie dla funkcjonalności single sign-on – po zalogowaniu w systemie operacyjnym użytkownik nie musi ponownie podawać ponownie nazwy użytkownika i hasła.

i. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów.

j. Dostępność wspieranego przez SKW sprzętu peryferyjnego. W tym telefonów IP pochodzących od różnych producentów.

Subskrypcja pakietu biurowego.

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

1. Wymagania odnośnie interfejsu użytkownika:
   - Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski,
   - Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
2. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory) – 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 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 nr 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 wykorzystanie schematów 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.

Pakiet zintegrowanych aplikacji biurowych musi zawierać:
- Edytor tekstów
- Arkusz kalkulacyjny
- Narzędzie do przygotowywania i prowadzenia prezentacji
- Narzędzie do tworzenia i wypełniania formularzy elektronicznych
- Narzędzie do tworzenia drukowanych materiałów informacyjnych
- Narzędzie do tworzenia i pracy z lokalną bazą danych
- Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
- Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR
- Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.

Edytor tekstów musi umożliwiać:
1. 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.
2. 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.
3. Wstawianie oraz formatowanie tabel.

4. Wstawianie oraz formatowanie obiektów graficznych.
5. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
6. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
7. Automatyczne tworzenie spisów treści.
8. Formatowanie nagłówków i stopek stron.
9. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
10. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
11. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
12. Określenie układu strony (pionowa/pozioma).
13. Wydruk dokumentów.
14. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
15. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
16. Zapis i edycję plików w formacie PDF.
17. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
18. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
19. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

Arkusz kalkulacyjny musi umożliwiać:

1. Tworzenie raportów tabelarycznych.
2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
7. Wyszukiwanie i zamianę danych.

8. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
9. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
11. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
12. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
13. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
14. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
15. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
16. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

1. Przygotowywanie prezentacji multimedialnych, które będą:
2. Prezentowanie przy użyciu projektora multimedialnego.
3. Drukowanie w formacie umożliwiającym robienie notatek.
4. Zapisanie jako prezentacja tylko do odczytu.
5. Nagrywanie narracji i dołączanie jej do prezentacji.
6. Opatrywanie slajdów notatkami dla prezentera.
7. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
8. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
9. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
10. Możliwość tworzenia animacji obiektów i całych slajdów.
11. 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.
12. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:

1. Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania.
2. Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków.

3. Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników.
4. Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych.
5. Możliwość pobierania danych z platformy do pracy grupowej.
6. Przesłanie danych przy użyciu usługi Web (tzw. web service).
7. Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.
8. Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.

Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
1. Tworzenie i edycję drukowanych materiałów informacyjnych.
2. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
3. Edycję poszczególnych stron materiałów.
4. Podział treści na kolumny.
5. Umieszczanie elementów graficznych.
6. wykorzystanie mechanizmu korespondencji seryjnej.
7. Płynne przesuwanie elementów po całej stronie publikacji.
8. Eksport publikacji do formatu PDF oraz TIFF.
9. Wydruk publikacji.
10. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.

Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
1. Tworzenie bazy danych przez zdefiniowanie:
2. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
3. Relacji pomiędzy tabelami.
4. Formularzy do wprowadzania i edycji danych.
5. Raportów.
6. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych.
7. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów.
8. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.

Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.

2. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
3. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
4. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
5. Automatyczne grupowanie poczty o tym samym tytule.
6. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
7. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
8. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
9. Zarządzanie kalendarzem.
10. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
11. Przeglądanie kalendarza innych użytkowników.
12. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
13. Zarządzanie listą zadań.
14. Zlecanie zadań innym użytkownikom.
15. Zarządzanie listą kontaktów.
16. Udostępnianie listy kontaktów innym użytkownikom.
17. Przeglądanie listy kontaktów innych użytkowników.
18. Możliwość przesyłania kontaktów innym użytkowników.

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

1. Pełna polska wersja językowa interfejsu użytkownika.
2. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
3. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory) – 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.
4. Możliwość obsługi tekstowych wiadomości błyskawicznych.
5. Możliwość komunikacji głosowej i video.

6. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
7. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
8. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

2.7. Prawo do uaktualniania serwera poczty elektronicznej typ I (licencja na serwer)

Serwer systemu poczty elektronicznej musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:
   a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.
   b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.
   c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami.
   d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia.
   e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
   f. Pełne wsparcie dla klienta poczty elektronicznej MS Outlook 2007 i nowszych wersji.
2. Funkcjonalność wspierająca pracę grupową:
   a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie.
   b. Możliwość określenia terminu wygaśnięcia wiadomości.
   c. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.
   d. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze.
   e. 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.
   f. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania.
   g. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań.
   h. Mechanizm udostępniania współdzielonych skrzynek pocztowych.
   i. Obsługa list i grup dystrybucyjnych.

j. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.

k. Możliwość informowania zewnętrznych użytkowników poczty elektronicznej o dostępności lub niedostępności.

l. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.

m. Widok rozmowy, automatycznie organizujący wątki wiadomości w oparciu o przebieg wymiany wiadomości między stronami.

n. Konfigurowalna 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.

o. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.

p. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.

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

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

s. Mechanizm automatycznego dostosowywania się funkcji wyszukiwania kontaktów do najczęstszych działań użytkownika skutkujący priorytetyzacją wyników wyszukiwania.

t. Możliwość wyszukiwania i łączenia danych (zgodnie z nadanymi uprawnieniami) z systemu poczty elektronicznej oraz innych systemów w organizacji (portali wielofunkcyjnych, komunikacji wielokanałowej i serwerów plików).

u. Możliwość dostępu do poczty elektronicznej i dokumentów przechowywanych w portalu wielofunkcyjnym z poziomu jednego interfejsu zarządzanego przez serwer poczty elektronicznej.

3. Funkcjonalność wspierająca zarządzanie systemem poczty:

a. Oparcie się o profile użytkowników usługi katalogowej Active Directory.

b. Wielofunkcyjna konsola administracyjna umożliwiająca zarządzanie systemem poczty oraz dostęp do statystyk i logów użytkowników.

c. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu.

d. Możliwość definiowania różnych limitów pojemności skrzynek dla różnych grup użytkowników.

e. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer.

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

g. Narzędzia kreowania, wdrażania i zarządzania politykami nazewnictwa grup dystrybucyjnych.

4. Utrzymanie bezpieczeństwa informacji.

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

   b. 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.

   c. Mechanizm zapobiegania wycieku danych ograniczający możliwość wysyłania danych poufnych do nieuprawnionych osób poprzez konfigurowalne funkcje monitoringu i analizy treści, bazujący na ustalonych politykach bezpieczeństwa.

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

   e. 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.

   f. Integracja z usługami zarządzania dostępem do treści 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. Wymagana jest możliwość użycia 2048-bitowych kluczy RSA, 256-bitowych kluczy SHA-1 oraz algorytmu SHA-2.

   g. Odbieranie wiadomości zabezpieczonych funkcją IRM przez zewnętrznych użytkowników oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.

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

   i. Wbudowane filtrowanie oprogramowania złośliwego, wirusów i oprogramowania szpiegującego zawartego w wiadomościach wraz z konfigurowalnymi mechanizmami powiadamiania o wykryciu i usunięciu takiego oprogramowania.

   j. Mechanizm audytu dostępu do skrzynek pocztowych z kreowaniem raportów audytowych.

5. Wsparcie dla użytkowników mobilnych:

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

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

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

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

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

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

6. Funkcje związane z niezawodnością systemu:

a. Zapewnienie pełnej redundancji serwerów poczty elektronicznej bez konieczności wdrażania klastrów oraz niezależnych produktów do replikacji danych.

b. Automatyzacja replikacji bazy danych i przełączania awaryjnego już dla dwóch serwerów poczty, a także w wypadku centrów danych rozproszonych geograficznie.

c. Utrzymanie dostępności i uzyskanie możliwości szybkiego odzyskiwania po awarii dzięki możliwości konfiguracji wielu replik każdej bazy danych skrzynki pocztowej.

d. Automatyczne odtwarzanie redundancji poprzez tworzenie kopii zapasowych w miejsce kopii na uszkodzonych dyskach według zadanego schematu.

e. Ograniczenie zakłócenia pracy użytkowników podczas przenoszenia skrzynek pocztowych między serwerami, pozwalające na przeprowadzanie migracji i konserwacji w dowolnym czasie – nawet w godzinach pracy biurowej.

f. Zapewnienie ochrony przed utratą e-maili spowodowaną uaktualnianiem lub awarią roli serwera transportu poprzez zapewnienie redundancji i inteligentne przekierowywanie poczty na inną dostępną ścieżkę.

2.8. Prawo do uaktualniania serwera poczty elektronicznej typ II (licencja na serwer)

Serwer systemu poczty elektronicznej musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:

a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.

b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.

c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami.

d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia.

e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.

f. Pełne wsparcie dla klienta poczty elektronicznej MS Outlook 2007 i nowszych wersji.

2. Funkcjonalność wspierająca pracę grupową:

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

b. Możliwość określenia terminu wygaśnięcia wiadomości.

c. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.

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

e. 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.

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

g. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań.

h. Mechanizm udostępniania współdzielonych skrzynek pocztowych.

i. Obsługa list i grup dystrybucyjnych.

j. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.

k. Możliwość informowania zewnętrznych użytkowników poczty elektronicznej o dostępności lub niedostępności.

l. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.

m. Widok rozmowy, automatycznie organizujący wątki wiadomości w oparciu o przebieg wymiany wiadomości między stronami.

n. Konfigurowalna 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.

o. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.

p. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.

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

r. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby wsparcia ze strony informatyków.
s. Mechanizm automatycznego dostosowywania się funkcji wyszukiwania kontaktów do najczęstszych działań użytkownika skutkujący priorytetyzacją wyników wyszukiwania.
t. Możliwość wyszukiwania i łączenia danych (zgodnie z nadanymi uprawnieniami) z systemu poczty elektronicznej oraz innych systemów w organizacji (portali wielofunkcyjnych, komunikacji wielokanałowej i serwerów plików).
u. Możliwość dostępu do poczty elektronicznej i dokumentów przechowywanych w portalu wielofunkcyjnym z poziomu jednego interfejsu zarządzanego przez serwer poczty elektronicznej.

3. Funkcjonalność wspierająca zarządzanie systemem poczty:
   a. Oparcie się o profile użytkowników usługi katalogowej Active Directory.
   b. Wielofunkcyjna konsola administracyjna umożliwiająca zarządzanie systemem poczty oraz dostęp do statystyk i logów użytkowników.
   c. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu.
   d. Możliwość definiowania różnych limitów pojemności skrzynek dla różnych grup użytkowników.
   e. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer.
   f. Możliwość korzystania interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.
   g. Narzędzia kreowania, wdrażania i zarządzania politykami nazewnictwa grup dystrybucyjnych.

4. Utrzymanie bezpieczeństwa informacji:
   a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym: śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, oraz archiwizacja danych.
   b. 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.
   c. Mechanizm zapobiegania wycieku danych ograniczający możliwość wysyłania danych poufnych do nieuprawnionych osób poprzez konfigurowalne funkcje monitoringu i analizy treści, bazujący na ustalonych politykach bezpieczeństwa.
   d. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości.
   e. 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.

f. Integracja z usługami zarządzania dostępem do treści 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. Wymagana jest możliwość użycia 2048-bitowych kluczy RSA, 256-bitowych kluczy SHA-1 oraz algorytmu SHA-2.

g. Odbieranie wiadomości zabezpieczonych funkcją IRM przez zewnętrznych użytkowników oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.

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

i. Wbudowane filtrowanie oprogramowania złośliwego, wirusów i oprogramowania szpiegującego zawartego w wiadomościach wraz z konfigurowalnymi mechanizmami powiadamiania o wykryciu i usunięciu takiego oprogramowania.

j. Mechanizm audytu dostępu do skrzynek pocztowych z kreowaniem raportów audytowych.

5. Wsparcie dla użytkowników mobilnych:

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

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

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

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

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

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

6. Funkcje związane z niezawodnością systemu:

   a. Zapewnienie pełnej redundancji serwerów poczty elektronicznej bez konieczności wdrażania klastrów oraz niezależnych produktów do replikacji danych.

b. Automatyzacja replikacji bazy danych i przełączania awaryjnego już dla dwóch serwerów poczty, a także w wypadku centrów danych rozproszonych geograficznie.

c. Utrzymanie dostępności i uzyskanie możliwości szybkiego odzyskiwania po awarii dzięki możliwości konfiguracji wielu replik każdej bazy danych skrzynki pocztowej.

d. Automatyczne odtwarzanie redundancji poprzez tworzenie kopii zapasowych w miejsce kopii na uszkodzonych dyskach według zadanego schematu.

e. Ograniczenie zakłócenia pracy użytkowników podczas przenoszenia skrzynek pocztowych między serwerami, pozwalające na przeprowadzanie migracji i konserwacji w dowolnym czasie – nawet w godzinach pracy biurowej.

f. Zapewnienie ochrony przed utratą e-maili spowodowaną uaktualnianiem lub awarią roli serwera transportu poprzez zapewnienie redundancji i inteligentne przekierowywanie poczty na inną dostępną ścieżkę.

g. Obsługa ponad pięciu baz danych.

2.9. System zarządzania środowiskami serwerowymi bez serwerowego systemu operacyjnego (licencja na 2 procesory)

Licencja oprogramowania zarządzania środowiskami serwerowymi musi być przypisana do każdego procesora fizycznego na serwerze zarządzanym. Oprogramowanie musi być licencjonowane na minimum 2 fizyczne procesory serwera zarządzanego. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Każda licencja na 2 fizyczne procesory serwera musi uprawniać do zarządzania 2 środowiskami systemu operacyjnego na tym serwerze.
Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

a. System zarządzania infrastrukturą i oprogramowaniem.

b. System zarządzania komponentami.

c. System zarządzania środowiskami wirtualnym.

d. System tworzenia kopii zapasowych.

e. System automatyzacji zarządzania środowisk IT.

f. System zarządzania incydentami i problemami.

g. Ochrona antymalware.

System zarządzania infrastrukturą i oprogramowaniem.

System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.

1. Inwentaryzacja i zarządzanie zasobami:

   a. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania.

   b. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu.

c. Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp.).

d. System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania.
System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta.

e. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera.

2. Użytkowane oprogramowanie – pomiar wykorzystania.

   a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania.

   b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.

3. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.

4. Definiowanie i sprawdzanie standardu serwera:

   a. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej.

   b. Reguły powinny sprawdzać następujące elementy systemy komputerowego:

      - stan usługi (Windows Service)
      - obecność poprawek (Hotfix)
      - WMI
      - rejestr systemowy
      - system plików
      - Active Directory
      - SQL (query)
      - Metabase

5. Raportowanie, prezentacja danych:

   a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub

   b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services.

   c. System powinien posiadać predefiniowane raport w następujących kategoriach:

      - Sprzęt (inwentaryzacja),
      - Oprogramowanie (inwentaryzacja),

- Oprogramowanie (wykorzystanie),
- Oprogramowanie (aktualizacje, w tym system operacyjny).

d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport.

e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu.

6. Analiza działania systemu, logi, komponenty.

a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy.

b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.

System zarządzania komponentami.

System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania:

1. Architektura.

a. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.

b. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.

c. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.

d. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.

e. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.

f. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.

g. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).

h. Wsparcie dla protokołu IPv6.

i. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta.

2. Audyt zdarzeń bezpieczeństwa.

System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować:

a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących).

b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji.

c. Obsługę co najmniej 2500 zdarzeń/sek. w trybie ciągłym i 100000 zdarzeń/sek. w trybie „burst" – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów.

3. Konfiguracja i monitorowanie.

System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:

a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:

- rejestru
- WMI
- OLEDB
- LDAP
- skrypty (uruchamiane w celu wykrycia atrybutów obiektu),

W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.

b. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp.

c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla:

- Windows Server 2003/2008/2008R2
- Active Directory 2003/2008
- Exchange 2003/2007/2010
- Microsoft SharePoint 2003/2007/2010
- Microsoft SharePoint Services 3.0
- Microsoft SharePoint Foundation 2010
- SQL 2005/2008/2008R2 (x86/x64/ia64)
- Windows Client OS (XP/Vista/7)
- Information Worker (Office, IExplorer, Outlook, itp…)
- IIS 6.0/7.0/7.5

- HP-UX 11i v2/v3
- Sun Solaris 9 (SPARC) oraz Solaris 10 (SPARC i x86)
- Red Hat Enterprise Linux 4/5/6 (x86/x64) Server
- Novell SUSE Linux Enterprise Server 9/10SP1/11
- IBM AIX v5.3 i v6.1/v7.1 (POWER)

d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.

e. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji:

- interfejsy sieciowe
- porty
- sieci wirtualne (VLAN)
- grupy Hot Standby Router Protocol (HSRP)

f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:

- SNMP (trap, probe)
- WMI Performance Counters
- Log Files (text, text CSV)
- Windows Events (logi systemowe)
- Windows Services
- Windows Performance Counters (perflib)
- WMI Events
- Scripts (wyniki skryptów, np.: WSH, JSH)
- Unix/Linux Service
- Unix/Linux Log

g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów.

4. Tworzenie reguł.

a. w systemie zarządzania powinna być możliwość czerpania informacji z następujących źródeł danych:

- Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event)
- Performance based (SNMP performance, WMI performance, Windows performance)
- Probe based (scripts: event, performance)

b. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia.

c. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości:

   - na ilość takich samych próbek o takiej samej wartości
   - na procentową zmianę od ostatniej wartości próbki.

d. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia" się monitorowanego parametru w zakresie przebiegu bazowego „baseline" w zadanym okresie czasu.

e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.

f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:

   - ASP .Net Application
   - ASP .Net Web Service
   - OLE DB
   - TCP Port
   - Web Application
   - Windows Service
   - Unix/Linux Service
   - Process Monitoring

   Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji

g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.

h. Z każdym elementem monitorującym (monitor, reguła, alarm, itp.) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu).

i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.

j. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla: monitora (dostępność), i licznika wydajności (z agregacją dla wartości – min, max, avg).

5. Przechowywanie i dostęp do informacji.

   a. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy itp.) powinny być przechowywane w bazie danych operacyjnych.

   b. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane.

   c. System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy).

   d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności.

   e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.

   f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:

      - XML
      - CSV
      - TIFF
      - PDF
      - XLS
      - Web archive

6. Konsola systemu zarządzania.

   a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.

   b. System powinien udostępniać dwa rodzaje konsoli:

      - w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna),
      - w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa).

   c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach:

      - Alerts
      - Events
      - State
      - Performance
      - Diagram
      - Task Status

- Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu).

d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.

e. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp.), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych".

f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.

g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:

- opcji definiowania ról użytkowników,
- opcji definiowania widoków,
- opcji definiowania i generowania raportów,
- opcji definiowania powiadomień,
- opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących,
- opcji instalacji/deinstalacji klienta.

h. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostępu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).

7. Wymagania dodatkowe.

a. System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na:

- Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo),
- Wykonywanie operacji w systemie z poziomu linii poleceń,
- Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania,
- Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie.

System zarządzania środowiskami wirtualnym.

System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy:

1. Architektura.

a. System zarządzania środowiskiem wirtualnym powinien składać się z:

- serwera zarządzającego,
- relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,

- konsoli, instalowanej na komputerach operatorów,
- portalu self-service (konsoli webowej) dla operatorów „departamentowych”,
- biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych,
- agenta instalowanego na zarządzanych hostach wirtualizacyjnych,
- „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych.

b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).

c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców.

2. Interfejs użytkownika.

a. Konsola musi umożliwiać wykonywanie codziennych zadań związanych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.

b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów.

c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp.

d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit.

e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.

3. Scenariusze i zadania.

a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:

i. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny.

ii. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:

- profilu sprzętowego,
- profilu systemu operacyjnego,
- przygotowanych dysków twardych.

b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.

c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:

- w trybie migracji „on-line” – bez przerywania pracy,
- w trybie migracji „off-line – z zapisem stanu maszyny.

d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.

e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.

f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance" w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu.

g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.

h. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji.

4. Wymagania dodatkowe.

a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę.

b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania.

c. System musi kreować raporty z działania zarządzanego środowiska, w tym:

- utylizacja poszczególnych hostów,
- trend w utylizacji hostów,
- alokacja zasobów na centra kosztów,
- utylizacja poszczególnych maszyn wirtualnych,
- komputery-kandydaci do wirtualizacji.

d. System musi umożliwiać skorzystanie z szablonów:

- wirtualnych maszyn,
- usług,

oraz profili dla:
- aplikacji,
- serwera SQL,
- hosta,
- sprzętu,
- systemu operacyjnego gościa.

e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).

f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.

g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją).

System tworzenia kopii zapasowych

System tworzenia i odtwarzania kopii zapasowych danych (backup) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych musi spełniać następujące wymagania:

1. System musi składać się z:
   a. serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych.
   b. agentów kopii zapasowych instalowanych na komputerach zdalnych.
   c. konsoli zarządzającej.
   d. relacyjnej bazy danych przechowującej informacje o zarządzanych elementach.
   e. wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną.
   f. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service).
2. System kopii zapasowych musi umożliwiać:
   a. zapis danych na puli magazynowej złożonej z dysków twardych.
   b. zapis danych na bibliotekach taśmowych.
3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej.
4. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe.
5. System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej.
6. Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania.
7. System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej pełnej kopii.
8. System kopii zapasowych powinien umożliwiać przywrócenie:
   a. danych plikowych.
   b. danych aplikacyjnych.
   c. stanu systemu (Systemstate).
   d. obrazu systemu operacyjnego (tzw. Bare Metal Restore).
9. System kopii zapasowej podczas wykonywania pełnej kopii zapasowej musi uaktualniać chronione dane o dodatkowy punkt przywracania danych, minimalizując ilość przesyłanych danych.
10. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji, wykorzystując przy tym mechanizm regulacji maksymalnej przepustowości.

11. Agenci systemu kopii zapasowych muszą posiadać konfiguracje dotyczącą zdefiniowania godzin pracy, a także dostępnej przepustowości w czasie godzin pracy i poza godzinami pracy.
12. System kopii zapasowych musi rozpoznawać aplikacje:
    a. ze względu na tworzone logi transakcyjne:
        - Microsoft Exchange Server
        - Microsoft Office Sharepoint Server
        - Microsoft SQL Server
    b. ze względu na zapewnienie nieprzerwalności pracy
        - Microsoft Virtual Server 2005
        - Microsoft Hyper-V server
13. Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach.
14. Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach.
15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów.
16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń.
17. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych przez użytkownika końcowego z poziomu zakładki „Poprzednie wersje".
18. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych.
19. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych.
20. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).
21. System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej do 1 roku.
22. System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 25 lat.
23. System kopii zapasowych musi umożliwiać synchronizacje przechowywanych kopii zapasowych (kopie inkrementalne) z produkcyjnymi transakcyjnymi bazami danych (bazy danych, poczta elektroniczna, portale intranetowe) na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
24. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych aplikacji, takich jak bazy transakcyjne, poczta elektroniczna, portale intranetowe.
25. System kopii zapasowych musi umożliwiać odtworzenie danych do:
    a. lokalizacji oryginalnej

b. lokalizacji alternatywnej

c. w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych.

System automatyzacji zarządzania środowisk IT

System automatyzacji zarządzania środowisk IT musi udostępniać bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk.

1. System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie.
2. System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT.
3. System musi wspomagać planowanie i automatyzację wdrażania poprawek.
4. System musi umożliwiać zarządzanie życiem środowisk wirtualnych.
5. System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania workflow.
6. Wbudowane konektory zapewniające integrację narzędzi Microsoft System Center, HP OpenView, IBM Tivoli i BMC Patrol do zarządzania oprogramowaniem i sprzętem.
7. Wbudowane (gotowe) workflow, takie jak:
   - Active Directory Password Reset
   - Microsoft Cluster Patching
   - Microsoft SQL Server Cluster Patching
   - Microsoft SQL: Server Dump Copy Load
   - Operations Manager Event Remediation
   - Operations Manager Event Remediation and Enrichment
   - Operations Manager Service Alert Testing
   - VM Provisioning
   - Working with FTP
   - Operations Manager Tool Integration
   - Operations Manager: Manager of Managers
   - Operations Manager: Maintenance Windows
   - Active Directory: New Employee Onboarding
   - Operations Manager: Multi-Service Desk Integration

System zarządzania incydentami i problemami

System zarządzania incydentami i problemami musi spełniać następujące wymagania:

1. System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na zasoby IT (np. nowa maszyna wirtualna).

2. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
3. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
4. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
5. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:
   - Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką,
   - Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia,
   - Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu,
   - Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,
   - Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów,
   - Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej,
   - Tworzenie baz wiedzy na temat rozwiązywania problemów,
   - Automatyzację działań w przypadku znanych i opisanych problemów,
   - Wykrywanie odchyleń od założonych standardów ustalonych dla systemu.

Ochrona antymalware

Oprogramowanie antymalware musi spełniać następujące wymagania:

1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem.
3. Centralne zarządzanie politykami ochrony.
4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
5. Mechanizmy wspomagające masową instalację.
6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów", skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.

7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.
8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa", itd.).
10. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.
11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu zasad grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

2.10. Serwerowy system operacyjny z elementami zarządzania z prawem do uaktualnienia (licencja na 2 procesory)

Licencja na serwerowy system operacyjny musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu.
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów.
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów.
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy.
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    a. Login i hasło.
    b. Karty z certyfikatami (smartcard).
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
19. Możliwość wymuszania wieloelementowej kontroli dostępu dla określonych grup użytkowników.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną.
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania.
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http.
        ii. Konsolidację CA dla wielu lasów domeny.
        iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
        iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f. Szyfrowanie plików i folderów.
    g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    i. Serwis udostępniania stron WWW.
    j. Wsparcie dla protokołu IP w wersji 6 (IPv6).
    k. Wsparcie dla algorytmów Suite B (RFC 4869).
    l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
    m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
        i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych.
        ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
        iii. Obsługi 4-KB sektorów dysków.

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra.
v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode).

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Licencja oprogramowania zarządzania środowiskami serwerowymi musi być przypisana do każdego procesora fizycznego na serwerze zarządzanym. Oprogramowanie musi być licencjonowane na minimum 2 fizyczne procesory serwera zarządzanego. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Każda licencja na 2 fizyczne procesory serwera musi uprawniać do zarządzania 2 środowiskami systemu operacyjnego na tym serwerze.
Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

a) System zarządzania infrastrukturą i oprogramowaniem
b) System zarządzania komponentami
c) System zarządzania środowiskami wirtualnym
d) System tworzenia kopii zapasowych
e) System automatyzacji zarządzania środowisk IT
f) System zarządzania incydentami i problemami
g) Ochrona antymalware

System zarządzania infrastrukturą i oprogramowaniem
System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.
1. Inwentaryzacja i zarządzanie zasobami:

a. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania.
b. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu.

c. Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp.).

d. System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta.

e. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera.

2. Użytkowane oprogramowanie – pomiar wykorzystania.

   a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania.

   b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.

3. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.

4. Definiowanie i sprawdzanie standardu serwera:

   a. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej.

   b. Reguły powinny sprawdzać następujące elementy systemy komputerowego:

      - stan usługi (Windows Service),
      - obecność poprawek (Hotfix),
      - WMI,
      - rejestr systemowy,
      - system plików,
      - Active Directory,
      - SQL (query),
      - Metabase.

5. Raportowanie, prezentacja danych:

   a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub

   b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services.

   c. System powinien posiadać predefiniowane raport w następujących kategoriach:

      - Sprzęt (inwentaryzacja),
      - Oprogramowanie (inwentaryzacja),

- Oprogramowanie (wykorzystanie),
- Oprogramowanie (aktualizacje, w tym system operacyjny).

d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport.

e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu.

6. Analiza działania systemu, logi, komponenty.

a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy.

b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.

System zarządzania komponentami

System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania:

1. Architektura.

a. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.

b. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.

c. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.

d. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.

e. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.

f. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.

g. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).

h. Wsparcie dla protokołu IPv6.

i. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta.

2. Audyt zdarzeń bezpieczeństwa.

System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować:

a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących).

b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji.

c. Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst" – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów.

3. Konfiguracja i monitorowanie.

System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:

a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:

   - rejestru
   - WMI
   - OLEDB
   - LDAP
   - skrypty (uruchamiane w celu wykrycia atrybutów obiektu),

   W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.

b. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp.

c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla:

   - Windows Server 2003/2008/2008R2
   - Active Directory 2003/2008
   - Exchange 2003/2007/2010
   - Microsoft SharePoint 2003/2007/2010
   - Microsoft SharePoint Services 3.0
   - Microsoft SharePoint Foundation 2010
   - SQL 2005/2008/2008R2 (x86/x64/ia64)
   - Windows Client OS (XP/Vista/7)
   - Information Worker (Office, IExplorer, Outlook, itp…)
   - IIS 6.0/7.0/7.5
   - HP-UX 11i v2/v3

- Sun Solaris 9 (SPARC) oraz Solaris 10 (SPARC i x86)
- Red Hat Enterprise Linux 4/5/6 (x86/x64) Server
- Novell SUSE Linux Enterprise Server 9/10SP1/11
- IBM AIX v5.3 i v6.1/v7.1 (POWER)

d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.

e. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji:
   - interfejsy sieciowe
   - porty
   - sieci wirtualne (VLAN)
   - grupy Hot Standby Router Protocol (HSRP)

f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:
   - SNMP (trap, probe)
   - WMI Performance Counters
   - Log Files (text, text CSV)
   - Windows Events (logi systemowe)
   - Windows Services
   - Windows Performance Counters (perflib)
   - WMI Events
   - Scripts (wyniki skryptów, np.: WSH, JSH)
   - Unix/Linux Service
   - Unix/Linux Log

g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów

4. Tworzenie reguł.

   a. W systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych:
      - Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event),
      - Performance based (SNMP performance, WMI performance, Windows performance),
      - Probe based (scripts: event, performance).

   b. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące

wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia.

c. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości:
   - na ilość takich samych próbek o takiej samej wartości,
   - na procentową zmianę od ostatniej wartości próbki.

d. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia" się monitorowanego parametru w zakresie przebiegu bazowego „baseline" w zadanym okresie czasu.

e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.

f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:
   - ASP .Net Application
   - ASP .Net Web Service
   - OLE DB
   - TCP Port
   - Web Application
   - Windows Service
   - Unix/Linux Service
   - Process Monitoring

   Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji

g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.

h. Z każdym elementem monitorującym (monitor, reguła, alarm, itp…) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu).

i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.

j. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla: monitora (dostepność), i licznika wydajności (z agregacją dla wartości – min, max, avg).

5. Przechowywanie i dostęp do informacji.

a. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp.) powinny być przechowywane w bazie danych operacyjnych.

b. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane.

c. System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy).

d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności.

e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.

f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:

   - XML
   - CSV
   - TIFF
   - PDF
   - XLS
   - Web archive

6. Konsola systemu zarządzania.

   a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.

   b. System powinien udostępniać dwa rodzaje konsoli:

      - w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna),
      - w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa).

   c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach:

      - Alerts
      - Events
      - State
      - Performance
      - Diagram
      - Task Status

- Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu).

d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.

e. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp…), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych".

f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.

g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:

- opcji definiowania ról użytkowników,
- opcji definiowania widoków,
- opcji definiowania i generowania raportów,
- opcji definiowania powiadomień,
- opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących,
- opcji instalacji/deinstalacji klienta.

h. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostępu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).

7. Wymagania dodatkowe.

a. System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na:

- budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo),
- wykonywanie operacji w systemie z poziomu linii poleceń,
- podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania,
- podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie.

System zarządzania środowiskami wirtualnym

System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy:

1. Architektura.

a. System zarządzania środowiskiem wirtualnym powinien składać się z:

- serwera zarządzającego,
- relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,
- konsoli, instalowanej na komputerach operatorów,

- portalu self-service (konsoli webowej) dla operatorów „departamentowych”,
- biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych,
- agenta instalowanego na zarządzanych hostach wirtualizacyjnych,
- „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych.

b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).

c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców.

2. Interfejs użytkownika.

a. Konsola musi umożliwiać wykonywanie codziennych zadań związanych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.

b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień posczególnym operatorom do grup hostów.

c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp.

d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit.

e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.

3. Scenariusze i zadania.

a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:

i. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny,

ii. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:

- profilu sprzętowego,
- profilu systemu operacyjnego,
- przygotowanych dysków twardych.

b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.

c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:

- w trybie migracji „on-line” – bez przerywania pracy,
- w trybie migracji „off-line – z zapisem stanu maszyny.

d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.

e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.

f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance" w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu.

g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.

h. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji.

4. Wymagania dodatkowe.

a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę.

b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania.

c. System musi kreować raporty z działania zarządzanego środowiska, w tym:

- utylizacja poszczególnych hostów,
- trend w utylizacji hostów,
- alokacja zasobów na centra kosztów,
- utylizacja poszczególnych maszyn wirtualnych,
- komputery-kandydaci do wirtualizacji.

d. System musi umożliwiać skorzystanie z szablonów:

- wirtualnych maszyn,
- usług,

oraz profili dla:

- aplikacji,
- serwera SQL,
- hosta,
- sprzętu,
- systemu operacyjnego gościa.

e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).

f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.

g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją).

System tworzenia kopii zapasowych

System tworzenia i odtwarzania kopii zapasowych danych (backup) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych musi spełniać następujące wymagania:

1. System musi składać się z:
    a. serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych.
    b. agentów kopii zapasowych instalowanych na komputerach zdalnych.
    c. konsoli zarządzającej.
    d. relacyjnej bazy danych przechowującej informacje o zarządzanych elementach.
    e. wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną.
    f. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service).
2. System kopii zapasowych musi umożliwiać:
    a. zapis danych na puli magazynowej złożonej z dysków twardych.
    b. zapis danych na bibliotekach taśmowych.
3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej.
4. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe.
5. System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej.
6. Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania.
7. System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej pełnej kopii.
8. System kopii zapasowych powinien umożliwiać przywrócenie:
    a. danych plikowych.
    b. danych aplikacyjnych.
    c. stanu systemu (Systemstate).
    d. obrazu systemu operacyjnego (tzw. Bare Metal Restore).
9. System kopii zapasowej podczas wykonywania pełnej kopii zapasowej musi uaktualniać chronione dane o dodatkowy punkt przywracania danych, minimalizując ilość przesyłanych danych.
10. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji, wykorzystując przy tym mechanizm regulacji maksymalnej przepustowości.

11. Agenci systemu kopii zapasowych muszą posiadać konfiguracje dotyczącą zdefiniowania godzin pracy, a także dostępnej przepustowości w czasie godzin pracy i poza godzinami pracy.
12. System kopii zapasowych musi rozpoznawać aplikacje:
    a. ze względu na tworzone logi transakcyjne:
        - Microsoft Exchange Server
        - Microsoft Office Sharepoint Server
        - Microsoft SQL Server
    b. ze względu na zapewnienie nieprzerwalności pracy
        - Microsoft Virtual Server 2005
        - Microsoft Hyper-V server
13. Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach.
14. Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach.
15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów.
16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń.
17. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych przez użytkownika końcowego z poziomu zakładki „Poprzednie wersje”.
18. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych.
19. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych.
20. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).
21. System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej do 1 roku.
22. System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 25 lat.
23. System kopii zapasowych musi umożliwiać synchronizacje przechowywanych kopii zapasowych (kopie inkrementalne) z produkcyjnymi transakcyjnymi bazami danych (bazy danych, poczta elektroniczna, portale intranetowe) na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
24. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych aplikacji, takich jak bazy transakcyjne, poczta elektroniczna, portale intranetowe.
25. System kopii zapasowych musi umożliwiać odtworzenie danych do:
    a. lokalizacji oryginalnej.

b. lokalizacji alternatywnej.

c. w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych.

System automatyzacji zarządzania środowisk IT

System automatyzacji zarządzania środowisk IT musi udostępniać bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk.

1. System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie.
2. System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT.
3. System musi wspomagać planowanie i automatyzację wdrażania poprawek.
4. System musi umożliwiać zarządzanie życiem środowisk wirtualnych.
5. System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania worklow.
6. Wbudowane konektory zapewniające integrację narzędzi Microsoft System Center, HP OpenView, IBM Tivoli i BMC Patrol do zarządzania oprogramowaniem i sprzętem.
7. Wbudowane (gotowe) workflow, takie jak:
   - Active Directory Password Reset
   - Microsoft Cluster Patching
   - Microsoft SQL Server Cluster Patching
   - Microsoft SQL: Server Dump Copy Load
   - Operations Manager Event Remediation
   - Operations Manager Event Remediation and Enrichment
   - Operations Manager Service Alert Testing
   - VM Provisioning
   - Working with FTP
   - Operations Manager Tool Integration
   - Operations Manager: Manager of Managers
   - Operations Manager: Maintenance Windows
   - Active Directory: New Employee Onboarding
   - Operations Manager: Multi-Service Desk Integration

System zarządzania incydentami i problemami

System zarządzania incydentami i problemami musi spełniać następujące wymagania:

1. System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na zasoby IT (np. nowa maszyna wirtualna).

2. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
3. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
4. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
5. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:
   - Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką,
   - Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia,
   - Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu,
   - Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,
   - Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów,
   - Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej,
   - Tworzenie baz wiedzy na temat rozwiązywania problemów,
   - Automatyzację działań w przypadku znanych i opisanych problemów,
   - Wykrywanie odchyleń od założonych standardów ustalonych dla systemu.

Ochrona antymalware

Oprogramowanie antymalware musi spełniać następujące wymagania:

1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem.
3. Centralne zarządzanie politykami ochrony.
4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
5. Mechanizmy wspomagające masową instalację.
6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów”, skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.

7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.
8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa", itd.).
10. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.
11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

2.11. Serwer portalu internet i intranet z prawem do uaktualnienia (licencja na serwer)

Serwery portali intranet i internet muszą realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy:

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych i zewnętrznych.
2. Zarządzanie strukturą portalu i treściami www.
3. Uczestnictwo Internautów 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. Udostępnienie formularzy elektronicznych.
6. Tworzenie repozytoriów wzorów dokumentów.
7. Tworzenie repozytoriów dokumentów.
8. Wspólną, bezpieczną pracę nad dokumentami.
9. Wersjonowanie dokumentów (dla wersji roboczych).
10. Organizację pracy grupowej.
11. Wyszukiwanie treści.
12. Dostęp do danych w relacyjnych bazach danych.
13. Analizy danych wraz z graficzną prezentacją danych.

14. Możliwość wykorzystanie mechanizmów portalu do budowy systemu zarządzania e-szkoleniami (e-learning).
15. 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.
16. PW 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 PW 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. Możliwość pracy off-line z plikami przechowywanymi w repozytoriach portalu.
   f. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
2. Uwierzytelnianie – wbudowane mechanizmy wspierające uwierzytelnianie na bazie:
   a. Oświadczeń (claim-based authentication) z wykorzystaniem:
      i. Open Authorization 2.0 dla uwierzytelniania aplikacji.
      ii. Uwierzytelniania w trybie server-to-server.
      iii. SAML.
      iv. Windows claims.
   b. Pojedynczego logowania domenowego (single-sign on),
   c. Na bazie formularzy (Form-based).
3. 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.
4. 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 systemem obsługującym serwis WWW w zakresie publikacji treści z repozytoriów wewnętrznych firmy na zewnętrzne strony serwisu WWW (pliki, strony).
e. 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.
f. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services.
g. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.
h. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

5. Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej przez autorów treści:
   a. Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania.
   b. Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów publikowanych w intranecie (stron HTML).
   c. Spójne zarządzanie wyglądem stron intranetu, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego.
   d. Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron intranetu i przechowywanymi w intranetowym repozytorium treści. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów.
   e. Definiowanie szablonów dla układów stron (tzw. layout'ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach intranetu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte.
   f. Możliwość wielokrotnego wykorzystania elementów zawartości intranetu (części treści publikowanych na stronach) w różnych częściach portalu, tzn. modyfikacja zawartości w jednym miejscu powoduje jej faktyczną zmianę na wszystkich stronach intranetu, gdzie dana treść została opublikowana.

g. Możliwość odwzorowania w systemie CMS przyjętej wizualizacji portalu intranetowego (projekt graficzny i funkcjonalny).
h. Możliwość osadzania na stronach narzędzia do odtwarzania materiałów audio i wideo.

6. Organizacja i publikacja treści:
   a. Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści.
   b. Zastosowanie procesów zatwierdzania zawartości przez publikacją, tzn. Udostępnieniem jej dla szerokiego grona pracowników. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed Udostępnieniem jej wszystkim użytkownikom intranetu.
   c. Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji.
   d. Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące obecną hierarchię.
   e. Automatyczne generowanie mapy stron portalu.
   f. Możliwość definiowania nawigacji w oparciu o centralne zarządzanie metadanymi.
   g. Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu.
   h. Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do odczytu zawartości, jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT.
   i. Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji.
   j. Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości, i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji.
   k. Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu oraz zapewnienie automatycznego tłumaczenia na wybrane języki.

7. Repozytoria dokumentów:
   a. Możliwość prostej publikacji dokumentów w intranecie przez edytorów portalu. Prosty sposób publikacji dokumentów, funkcjonalny dostęp użytkowników intranetu do opublikowanych dokumentów.
   b. Wykorzystanie do publikacji, edycji i przeglądania dokumentów w repozytorium narzędzi znanych użytkownikom np. pakiety biurowe czy przeglądarka internetowa.
   c. Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu.
   d. Możliwość publikacji plików w strukturze katalogów.
   e. Możliwość publikacji materiałów wideo oraz audio.

f. Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku.
g. Możliwość nawigacji po repozytorium dokumentów (lub całym portalu) w oparciu o metadane z metryk dokumentów.
h. Prosty, elastyczny i niezależny od działu IT mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania.
i. Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x… 2.0), automatyczna kontrola wersji przy publikacji dokumentów.
j. Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub modyfikowanych dokumentów. System informuje użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i pozwala podjąć decyzję o ich publikacji lub odrzuceniu.
k. Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych.
l. Możliwość definiowania polityk cyklu życia dokumentu oraz retencji dokumentów.
m. Możliwość tworzenia specjalnych repozytoriów przeznaczonych na raporty osadzone w arkuszach kalkulacyjnych w formacie ISO/IEC 29500:2008. Serwer powinien generować na podstawie tych arkuszy kalkulacyjnych raporty dostępne do oglądania przez przeglądarkę Internetową bez zainstalowanych innych narzędzi klienckich.
n. Możliwość automatyzacji usuwania duplikatów dokumentów.

8. Wyszukiwanie treści:
   a. Pełnotekstowe indeksowanie zawartości intranetu w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez webservice.
   b. Centralny mechanizm wyszukiwania treści dostępny dla użytkowników intranetu
   c. Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, oraz zakresów dat publikacji.
   d. Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów intranetu wg zadanych kryteriów, np. wg typów dokumentów.
   e. Możliwość definiowania słownika słów wykluczonych (często używanych).
   f. Możliwość tworzenia „linków sponsorowanych”, prezentowanych wysoko w wynikach wyszukiwania w zależności od słów wpisanych w zapytaniu.
   g. Podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu.
   h. Przedstawianie w wynikach duplikatów plików.
   i. Statystyki wyszukiwanych fraz.
9. Administracja intranetem i inne funkcje:
   a. Możliwość definiowania ról / grup uprawnień, w ramach których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami dostępna dla administratorów merytorycznych intranetu, niewymagająca szczególnych kompetencji technicznych.

b. Możliwość określania uprawnień do poszczególnych elementów zawartości intranetu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu.
c. Generowanie powiadomień pocztą elektroniczną dla użytkowników intranetu z informacją o publikacji najbardziej istotnych treści.
d. Definiowanie metryk opisujących dokumenty w poszczególnych repozytoriach portalu oraz centralnie zarządzanego zbioru metadanych z wyznaczonym administratorem merytorycznym.
e. Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i webservice oraz wykorzystywania ich do opisywania dokumentów.
f. Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów intranetu.
g. Statystyki odwiedzin poszczególnych części i stron intranetu – analiza liczby odsłon w czasie. Opcjonalnie zaawansowane statystyki i analizy.
h. Funkcjonalności wspierające pracę grupową - do wykorzystania na najniższym poziomie intranetu do celów pracy działów i zespołów zadaniowych. Funkcjonalności wspierające gromadzenie dokumentów, wsparcie komunikacji, planowanie zadań i wydarzeń.
i. Funkcjonalność publikowania na portalu formularzy elektronicznych XML i przetwarzanych na aplikację webową dostępną dla użytkowników przez przeglądarkę Internetową. Dane z wypełnionego formularza mają być zapisywane w formacie XML zgodnie z definicją formularza.
j. Mechanizmy wspierające przepływy pracy (workflow) wraz z funkcjonalnością definiowania procesów obiegu dokumentów, integracji przepływów z web-services, wywoływania web-services z poziomu workflow bez konieczności kodowania przy wykorzystaniu prostych w obsłudze narzędzi portalu.

2.12. Serwer komunikacji wielokanałowej z prawem do uaktualnienia (licencja na serwer)

System oparty na funkcjonalności serwera komunikacji wielokanałowej (SKW) wspomagający wewnętrzną komunikację Zamawiającego ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

1. Prostą, efektywną kosztowo, niezawodną i bezpieczną komunikację głosową oraz video.
2. Przesyłanie wiadomości błyskawicznych (tekstowych) z komputerów klasy PC wyposażonych w klienta SKW lub przeglądarkę.
3. Możliwość organizowania telekonferencji.

Wymagana jest funkcjonalność polegająca na umożliwieniu współpracy wykorzystującej integrację poczty elektronicznej, kalendarzy, wiadomości błyskawicznych, konferencji w sieci Web, audio i wideokonferencji. Serwer SKW ma zapewniać integrację z komponentami portalu wielofunkcyjnego i poczty elektronicznej. Ponadto SKW będzie wykorzystywała mechanizm pojedynczego logowania (single sign-on), uprawnień użytkowników i ich grup, bazując na komponencie posiadanych usług katalogowych (Active Directory). Wynikiem takiej integracji mają być następujące cechy systemu:

1. Ujednolicenie komunikacji biznesowej.

a. Dostęp z dowolnego miejsca do komunikacji w czasie rzeczywistym i asynchronicznej.
b. Możliwość ujednolicenia i współdziałania poczty głosowej, e-mail, kontaktów, kalendarzy, wiadomości błyskawicznych (IM) i danych o obecności.
c. Dostępność aplikacji klienckiej udostepniającej komunikację głosową, video i tekstową, organizowanie konferencji planowanych i ad-hoc.
d. Dostępność aplikacji klienckiej dla uczestników telekonferencji nieposiadających licencji dostępowej do serwerów SKW z funkcjonalnością:
   - 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,
   - Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji.
e. Dostępność funkcjonalności text-to-speech w języku polskim.
f. Integracja z aplikacjami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
g. Wbudowane mechanizmy dostępu mobilnego i bezprzewodowego.
h. Rozszerzalna platforma integracji narzędzi współpracy z pakietem biurowym.
i. Usługi bezpieczeństwa umożliwiające chronioną komunikację wewnątrz organizacji.
j. Aplikacje biznesowe dostępne bezpośrednio na urządzeniach mobilnych.
k. Mobilny dostęp do ludzi i danych firmowych.
l. Obniżone koszty dzięki zdalnej administracji i zarządzaniu urządzeniami.
m. Niższe koszty usług telefonicznych i komunikacji między odległymi lokalizacjami.
n. Funkcje statusu obecności, IM i konferencji (głosowych i video) bezpośrednio wbudowane w portale i obszary robocze zespołów i dostępne z poziomu klienta poczty elektronicznej.
o. Możliwość wspólnej pracy zespołów z różnych lokalizacji, wewnątrz i spoza ram organizacyjnych, także z wykorzystaniem przez użytkowników zewnętrznych bezpłatnych aplikacji klienckich.

2. W związku z tak postawionymi założeniami SKW ma zapewnić:
   a. Efektywną wymianę informacji z możliwością wyboru formy i kanału komunikacji i niezależnie od lokalizacji pracowników.
   b. Ulepszoną komunikację poprzez wykorzystanie statusu obecności i konferencje w czasie rzeczywistym.
   c. Zarządzanie, sortowanie i pracę z różnymi typami wiadomości, bez konieczności przełączania się pomiędzy aplikacjami czy systemami.
   d. Dostęp z dowolnego miejsca poprzez dostęp do usług komunikacyjnych z poziomu pulpitu, przeglądarki sieci Web i urządzeń mobilnych.
3. SKW ma zapewnić obsługę następujących funkcjonalności:
   a. Status obecności – informacja o statusie dostępności użytkowników (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej, zintegrowana z usługą katalogową i kalendarzem, a dostępna w interfejsach poczty elektronicznej, komunikatora i portalu wielofunkcyjnego. Wymagana jest

możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności.

b. Krótkie wiadomości tekstowe – Możliwość komunikacji typu chat. Możliwość grupowania kontaktów, możliwość konwersacji typu jeden-do-jednego, jeden-do-wielu, możliwość rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat. Możliwość komunikacji z darmowymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu. Możliwość administracyjnego zarządzania treściami przesyłanymi w formie komunikatów tekstowych.
c. Obsługa komunikacji głosowej – Możliwość realizowania połączeń głosowych między użytkownikami lokalnymi, możliwość realizacji połączeń głosowych do i z sieci PSTN (publicznej sieci telefonicznej). Możliwość realizacji funkcjonalności RCC (Remote Call Controll) tj. zarządzania telefonem stacjonarnym firm trzecich z poziomu komunikatora.
d. Obsługa komunikacji wideo – Możliwość zestawiania połączeń wideo-telefonicznych.
e. Obsługa konferencji wirtualnych – Możliwość realizacji konferencji wirtualnych z wykorzystaniem głosu i wideo. Możliwość współdzielenia aplikacji jak również całego pulpitu.
f. Możliwość dostępu do telekonferencji użytkownikom wykorzystujących urządzenia z systemami Android, Apple iOS, Windows, Windows Phone.
g. Możliwość nagrywania konferencji na centralnym serwerze jak również lokalnie przez uczestników.
h. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie z poziomu serwera WWW.
i. Automatyzacja planowania konferencji - zaproszenia rozsyłane są automatycznie w postaci poczty elektronicznej.
j. Wsparcie dla funkcjonalności single sign-on – po zalogowaniu w systemie operacyjnym użytkownik nie musi ponownie podawać ponownie nazwy użytkownika i hasła.
k. Wbudowane funkcjonalności: SIP Proxy.
l. Wbudowana funkcjonalność mostka konferencyjnego MCU.
m. Obsługa standardów: CSTA, TLS, SIP over TCP.
n. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów.
o. Kodowanie video H.264.
p. Wsparcie dla adresacji IPv6.
q. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności.
r. Wykorzystanie wyłącznie 64 bitowej platformy serwerowego systemu operacyjnego.
s. Możliwość instalacji w układzie klastra niezawodnościowego.
t. Dostępność wspieranego przez SKW sprzętu peryferyjnego. W tym telefonów IP pochodzących od różnych producentów.

4. Wymagania w zakresie administracji i zarządzania serwerem:
   a. Mechanizm pozwalający na przełączenie serwera w tryb off-line (np. w celach dokonania czynności administracyjnych) bez utraty usług serwera dla zalogowanych użytkowników, a jednocześnie blokujący dostęp nowych użytkowników.
   b. Możliwość administrowania z wiersza poleceń.
   c. Możliwość administrowania za pomocą interfejsu Web.

d. Mechanizm gotowych kreatorów (wizard) umożliwiających planowanie i zmiany topologii serwerów SKW.
e. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników.

5. Dodatkowe wymagania.
   a. Możliwość instalacji w układzie klastra typu load-balancing.
   b. DNS load balancing balansujący ruch sieciowy dla serwerów SKW, na przykład w zakresie ruchu SIP lub mediów.
   c. Możliwość instalacji bazy danych serwera komunikacji wielokanałowej na oddzielnym serwerze.
   d. Możliwość wydzielenia na niezależnym serwerze roli serwera konferencji audio i video.

2.13. Prawo do uaktualniania serwera bazy danych (licencja na 2 rdzenie procesora)

System bazodanowy (SBD) musi spełniać następujące wymagania poprzez wbudowane mechanizmy:

1. Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
5. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
6. SBD musi umożliwiać tworzenie klastrów niezawodnościowych.
7. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:
   - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
   - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
   - klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,

8. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
9. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.
10. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.
11. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń:
    - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),
    - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),
    - para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).
12. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
13. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków" obiektu, „rodzica" itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.
14. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:
    - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
    - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
    - udostępniać język zapytań do struktur XML,
    - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
    - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.

15. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:
    - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
    - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
    - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
    - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).
16. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System powinien umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo powinien udostępniać środowisko do debuggowania.
17. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
18. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
19. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.
20. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.
21. System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:
    - mechanizm debuggowania tworzonego rozwiązania,
    - mechanizm stawiania „pułapek” (breakpoints),
    - mechanizm logowania do pliku wykonywanych przez transformację operacji,

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

22. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.
23. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).
24. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
25. Wbudowany system analityczny powinien posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
26. Wbudowany system analityczny powinien obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
27. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system powinien udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
28. System analityczny powinien pozwalać na dodawanie własnych algorytmów oraz modułów wizualizacji modeli Data Mining.
29. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych

zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.

30. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania powinien obsługiwać:
    - raporty parametryzowane,
    - cache raportów (generacja raportów bez dostępu do źródła danych),
    - cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),
    - współdzielenie predefiniowanych zapytań do źródeł danych,
    - wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
    - możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
    - możliwość wizualizacji wskaźników KPI,
    - możliwość wizualizacji danych w postaci obiektów sparkline.
31. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
32. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel (od wersji 1997 do 2010), Microsoft Word (od wersji 1997 do 2010), HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.
33. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.
34. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).
35. Wbudowany system raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.

2.14. Prawo do uaktualniania pakietu zarządzania projektami

Pakiet zarządzania projektami ma zapewnić 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.
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.

2.15. Pakiet zarządzania projektami z prawem do uaktualniania

Pakiet zarządzania projektami ma zapewnić 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.
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.

2.16. Prawo do uaktualniania pakietu modelowania graficznego

Narzędzie do 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. Możliwość importu i eksportu do formatu plików zgodnych z AutoCad.
3. Możliwość graficznego obrazowania i analizowania danych pobieranych z plików xls i xlsx, baz danych dostępnych przez ODBC na diagramach.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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. Możliwość automatycznego modyfikowania raportów w miarę zmian informacji o projektach.

2.17. Pakiet modelowania graficznego z prawem do uaktualniania

Narzędzie do 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. Możliwość importu i eksportu do formatu plików zgodnych z AutoCad.
3. Możliwość graficznego obrazowania i analizowania danych pobieranych z plików xls i xlsx, baz danych dostępnych przez ODBC na diagramach.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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. Możliwość automatycznego modyfikowania raportów w miarę zmian informacji o projektach.

2.18. Platforma usług hostowanych

Platforma usług hostowanych ma być osadzona na standardowej, powszechnie dostępnej poprzez internet na zasadzie subskrypcji, skalowalnej i bezpiecznej usłudze polegającej na udostępnieniu serwerowej platformy umożliwiającej osadzanie własnych aplikacji.
Usługa ta powinna się cechować następującymi parametrami:

1. Usługa musi być dostępna przez okres 12 miesięcy od jej uruchomienia.
2. Minimum 100 000 godzin czasu obliczeniowego w ciągu miesiąca dla znormalizowanej jednostki obliczeniowej (1 rdzeń procesora 1.5GHz, 1.5 GB pamięci operacyjnej).
3. Dostęp do przestrzeni dyskowej o sumarycznej pojemności minimum 45 TB.
4. Minimum 4TB transferu danych miesięcznie.
5. Wsparcie techniczne z gwarantowanym czasem reakcji.
6. Dostępność usługi na poziomie 99,9%.
7. Możliwość skalowania usługi.
8. Możliwość dynamicznego zwiększania i zmniejszania zasobów sprzętowych bez przestoju pracy aplikacji.
9. Wdrażanie nowych wersji aplikacji bez przestoju działających wersji.
10. Automatyczna, nie wpływająca na ciągłość pracy systemu instalacja poprawek udostępnianych przez dostawcę systemu operacyjnego.

11. Możliwość gromadzenia i przetwarzania danych w udostępnianej przez platformę bazie relacyjnej, w oparciu o składnię SQL.
12. Łatwa integracja z wdrożonymi lokalnie usługami katalogowymi, zgodnie ze specyfikacją WS-Federation.
13. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP .
14. Możliwość uruchomienia aplikacji internetowych wykorzystujących technologię ASP.NET z automatyczną dystrybucją ruchu sieciowego HTTP pomiędzy kilka pracujących serwerów.
15. Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów z możliwością zdalnego dostępu.
16. Platforma ma korzystać z serwerowych systemów operacyjnych zgodnych z opisanymi w specyfikacji.

2.19. Pakiet usług standardowych opieki serwisowej do oprogramowania będącego przedmiotem dostawy

Pakiet usług musi obejmować swoim zakresem świadczenie opieki serwisowej do posiadanego i zamawianego oprogramowania w okresie 36 miesięcy.
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 certyfikowanego specjalisty 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 powyżej czas reakcji.
Wymagane jest zapewnienie opieki serwisowej nad dostarczonym oprogramowaniem na następujących zasadach:

1. Wykonawca będzie świadczyć usługi w zakresie organizacji i koordynacji usług w zakresie wsparcia technicznego oprogramowania wyprodukowanego przez producenta oprogramowania lub spółki zależne producenta (Producenta).

2. Wsparcie dotyczyć będzie oprogramowania będącego przedmiotem niniejszego postępowania (Produktów), z zastrzeżeniem pkt. 6 d) i e).
3. Usługi w zakresie wsparcia technicznego będą świadczone przez okres 36 miesięcy od dnia zawarcia umowy. Po upływie 26 miesięcy trwania umowy Zamawiający podejmie decyzję o przedłużeniu umowy o kolejne 12 lub 36 miesięcy na podstawie oddzielnego postępowania o udzielenie zamówienia publicznego.
4. Wykonawca zapewni możliwość bezpośredniego zgłaszania problemów technicznych przez Zamawiającego do producenta oprogramowania lub spółki zależnej producenta (Producenta) drogą elektroniczną poprzez dedykowaną stronę producenta i telefonicznie.
5. Wykonawca zagwarantuje możliwość wykonywania poprawek do oprogramowania (HotFix) przez Producenta.
6. Warunki świadczenia usług w zakresie wsparcia technicznego Produktów:
   a. Usługi w zakresie wsparcia technicznego w zakresie Produktów mają obejmować:
      - usługi reaktywne, czyli 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),
      - usługi proaktywne, czyli usługi mające 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.
   b. 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.
   c. W ramach usług wsparcia technicznego Zamawiający wymaga przedstawienia oferty na standardowe pakiety wsparcia technicznego zawierające:
      - 480 godzin roboczych działań proaktywnych (do 160 godzin rocznie) – związanych z zapobieganiem problemom,
      - 420 godzin roboczych reaktywnych (do 140 godzin rocznie) – związanych z rozwiązywaniem zgłoszonych problemów technicznych możliwych do wykorzystania w okresie trwania umowy.

      W przypadku, gdy godziny reaktywne nie byłyby wykorzystane, musi istnieć możliwość konwersji ich na godziny usług proaktywnych.
   d. 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.
   e. 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.
   f. 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 zgłoszeń wszystkich Problemów) lub zgłaszane w formie elektronicznej na dedykowanym dla

Zamawiającego serwisie internetowym (dla zgłoszeń Problemów 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.

g. 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. Lista lokalizacji Zamawiającego stanowi załącznik do specyfikacji.

h. Wykonawca zapewni regularne przekazywanie Zamawiającemu przez Producenta informacji technicznych w postaci biuletynu technicznego osobom kontaktowym wskazanym przez Zamawiającego.

i. 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 zawarcia 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.

j. Po zawarciu umowy w zakresie usług wsparcia technicznego, w uzgodnionym terminie, przedstawiciel Producenta przeprowadzi, po ustaleniu terminu z Zamawiającym, 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.

Rozdział III
ISTOTNE POSTANOWIENIA UMOWY

§ 1.

1. Przedmiotem zamówienia jest dostawa dla GDDKIA nowych licencji, aktualizacja już posiadanych licencji oraz wsparcie techniczne i opieka serwisowa producenta oprogramowania przez okres 36 miesięcy od daty zawarcia umowy, zgodnie ze Specyfikacją Istotnych Warunków Zamówienia stanowiącą załącznik nr 3 do Umowy oraz Ofertą Wykonawcy (załącznik nr 4 do Umowy).
2. Prawo eksploatacji oprogramowania i korzystania z opieki serwisowej przysługuje Zamawiającemu we wszystkich lokalizacjach wskazanych w OPZ oraz w wymienione w Załączniku nr 1 do Umowy.
3. Wykonawca nie później niż w czasie 14 dni po zawarciu umowy dostarczy Zamawiającemu do Centrali GDDKiA nośniki z wersją instalacyjną oraz klucze aktywacyjne, a także dokumenty niezbędne do uruchomienia dostępu do oprogramowania i uprawniające do korzystania z licencji.
4. Wykonawca wyznacza dedykowanego i uprawnionego specjalistę, który będzie odpowiedzialny za realizację usług wsparcia technicznego, a także za przekazywanie oraz otrzymywanie informacji i komentarzy zwrotnych dotyczących świadczonych usług: ……., tel. ……, e-mail: ……..
5. Zamawiający wyznacza ze swojej strony osobę uprawnioną do kontaktów z wyznaczonym specjalistą, o którym mowa w ust. 4, w tym składania zgłoszeń oraz koordynowania działań w ramach wsparcia technicznego: ……., tel. ……, e-mail: ……..
6. Osobą uprawnioną do nadzoru nad realizacją niniejszej umowy jest Dyrektor Departamentu Informacji i Informatyki, …….
7. Zmiana danych, o których mowa w ust. 4 - 6 nie stanowi zmiany Umowy.
8. Zamówienie jest finansowane ze środków budżetowych oraz częściowo w ramach Pomocy Technicznej Programu Operacyjnego Infrastruktura i Środowisko (POIiŚ) będących w dyspozycji Generalnego Dyrektora Dróg Krajowych i Autostrad.

§ 2

1. Wykonawca oświadcza, że posiada uprawnienia do sprzedaży licencji objętego umową oprogramowania.
2. Wykonawca zabezpieczy Zamawiającego od jakichkolwiek roszczeń osób trzecich odnośnie naruszenia ich praw, w szczególności autorskich, w czasie lub w związku z realizacją przedmiotu umowy.
3. Wykonawca zobowiązuje się wykonywać umowę z najwyższą starannością, zgodnie z ofertą i obowiązującymi przepisami prawa, a w szczególności odpowiada za jakość i terminowość wykonania umowy.
4. Wykonawca zobowiązany jest zapewnić wykonanie umowy przez osoby, posiadające odpowiednie kwalifikacje zawodowe i doświadczenie.
5. Wykonawca odpowiada za działania i zaniechania podwykonawców oraz osób, za pomocą których wykonuje umowę, jak za własne działania i zaniechania.
6. Wykonawca zobowiązany jest do niezwłocznego informowania Zamawiającego o wszystkich zdarzeniach mających lub mogących mieć wpływ na wykonanie umowy, w tym o wszczęciu wobec niego postępowania egzekucyjnego, naprawczego, likwidacyjnego lub innego, a także o innych istotnych zdarzeniach, w szczególności ogłoszeniu upadłości – następnego dnia od dnia jej ogłoszenia.

§ 3.

1. Strony ustalają opłatę za cały okres trwania Umowy w wysokości …….. zł netto (słownie złotych : ……), a wraz z podatkiem VAT 23 % wynosi …….. zł brutto (słownie złotych: ……).
2. Kwota, o której mowa w ust. 1 płatna będzie w 3 (trzech) rocznych ratach:

   1) Pierwsza roczna rata stanowić będzie 20% kwoty brutto …… zł (słownie złotych: ……) wymienionej w ust. 1.

   2) Druga roczna rata stanowić będzie 40% kwoty brutto …… zł (słownie złotych: ……) wymienionej w ust. 1.

   3) Trzecia roczna rata stanowić będzie 40% kwoty brutto …… zł (słownie złotych: ……) wymienionej w ust. 1.
3. Podstawą do wystawienia każdej faktury VAT za realizację przedmiotu umowy jest podpisany przez obie Strony protokół odbioru potwierdzający należyte wykonanie umowy. Wzór protokołu stanowi załącznik nr 2 do umowy.
4. Protokół, o którym mowa w ust. 3, ze strony Zamawiającego podpisuje Dyrektor Departamentu Informacji i Informatyki, ze strony Wykonawcy ……..
5. Zapłata wynagrodzenia nastąpi przelewem na rachunek bankowy Wykonawcy ……., w terminie 21 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury wraz z podpisanym przez przedstawicieli Stron protokołem odbioru, o którym mowa w ust. 3.
6. Za datę zapłaty Strony ustalają dzień, w którym Zamawiający wydał swojemu bankowi polecenie przelewu wynagrodzenia na rachunek bankowy Wykonawcy.
7. Określone powyżej wynagrodzenie obejmuje wszelkie koszty i wydatki związane z wykonaniem niniejszej umowy i wyczerpuje wszelkie roszczenia wykonawcy z niej wynikające, w tym z tytułu przeniesienia licencji na zasadach i w każdym przypadku określonym w umowie.

§ 4.

Wykonawca zobowiązuje się przekazać Zamawiającemu nośniki z oprogramowaniem będącym przedmiotem Umowy w terminie 14 dni od dnia zawarcia umowy, zaś aktualizacje co 30 dni (jeśli będą dostępne).

§ 5.

Jeżeli w nośnikach z wersją instalacyjną oprogramowania ujawnią się wady Zamawiający może wyznaczyć Wykonawcy pisemnie termin do ich usunięcia nie krótszy niż 21 dni i nie dłuższy niż 28 dni, a po jego bezskutecznym upływie może od umowy odstąpić. Odstąpienie od umowy w takim przypadku uznawane jest za dokonane z winy Wykonawcy.

§ 6.

1. Wykonawca zapłaci Zamawiającemu karę umowną:

   1) w przypadku opóźnienia w realizacji przedmiotu umowy w terminie, o którym mowa w § 1 ust. 3, Wykonawca zobowiązany jest do zapłacenia Zamawiającemu kary umownej w wysokości 0,1% wartości brutto przedmiotu umowy określonej w § 3 ust. 1, za każdy dzień zwłoki;

   2) w przypadku odstąpienia od Umowy na skutek okoliczności, za które odpowiedzialność ponosi Wykonawca – w wysokości 20% wartości brutto przedmiotu umowy określonej w § 3 ust. 1.
2. Jeżeli kara umowna nie pokrywa poniesionej szkody, Zamawiający może dochodzić odszkodowania uzupełniającego w wysokości przewyższającej karę umowną

§ 7.

1. Strony nie ponoszą odpowiedzialności za niewykonanie lub nieprawidłowe wykonanie umowy z powodu siły wyższej.
2. Przez siłę wyższą, o której mowa w § 5 ust. 3, rozumie się zdarzenia niemożliwe do przewidzenia, na które strony nie mają wpływu i są przez strony niemożliwe do pokonania, a w szczególności: klęski żywiołowe, wojny, mobilizacje, zamknięcie granic uniemożliwiające wykonanie umowy w całości lub części.
3. Strona może powołać się na zaistnienie siły wyższej tylko wtedy, gdy poinformuje o tym pisemnie drugą stronę w ciągu 2 dni roboczych od powstania tych okoliczności.
4. Ciężar udowodnienia okoliczności zaistnienia siły wyższej, w tym okresu jej trwania, spoczywa na stronie, która się na nie powołuje.

§ 8

Strony zobowiązują się do utrzymania w tajemnicy wszelkich informacji handlowych i innych informacji o poufnym charakterze dotyczących wykonania umowy lub uzyskanych od siebie w związku z jej wykonywaniem i zobowiązują się do nie ujawniania tych informacji bez pisemnej zgody drugiej strony, chyba że obowiązek ujawnienia tych informacji wynika z przepisów prawa, lub informacje te są powszechnie znane. Obowiązek zachowania tajemnicy trwa także po wygaśnięciu umowy.

§ 9.

1. W przypadku zmiany ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2011 r. nr 177, poz. 1054 z późn. zm.) w zakresie procentowej stawki podatku VAT, wartość umowy zostanie odpowiednio dostosowana aneksem do tych zmian.
2. Każda zmiana postanowień niniejszej Umowy może nastąpić jedynie w formie pisemnej pod rygorem nieważności.

§ 10.

Realizacja niniejszej umowy nie wiąże się z powierzeniem Wykonawcy przetwarzania danych osobowych, których administratorem jest Generalny Dyrektor Dróg Krajowych i Autostrad.

§ 11.

1. Wszelkie spory wynikające z niniejszej Umowy lub powstające w związku z jej stosowaniem, sprawy dotyczące naruszenia, rozwiązania lub ważności umowy, Strony Umowy poddają rozpoznaniu przez sąd powszechny właściwy dla siedziby Zamawiającego.
2. W sprawach nieuregulowanych niniejszą umową zastosowanie mają przepisy Kodeksu cywilnego i ustawy Prawo zamówień publicznych oraz ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym egzemplarzu dla każdej Strony.
4. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej, pod rygorem nieważności za zgodą obu Stron.
5. Integralną częścią umowy są załączniki:

Załącznik nr 1 - Wykaz jednostek organizacyjnych zamawiającego

Załącznik nr 2 - Wzór protokołu odbioru

Załącznik nr 3 - Specyfikacja Istotnych Warunków Zamówienia

Załącznik nr 4 – Oferta Wykonawcy

Załącznik nr 1 do Umowy

WYKAZ JEDNOSTEK ORGANIZACYJNYCH ZAMAWIAJĄCEGO

Lp.	Nazwa jednostki organizacyjnej	Adres
1.	Centrala GDDKiA	00-874 Warszawa, ul. Wronia 53
2.	GDDKiA Oddział w Białymstoku	15-703 Białystok, ul. Zwycięstwa 2
3.	GDDKiA Oddział w Bydgoszczy	85-085 Bydgoszcz, ul. Fordońska 6
4.	GDDKiA Oddział w Gdańsku	80-354 Gdańsk, ul. Subisława 5
5.	GDDKiA Oddział w Katowicach	40-016 Katowice, ul. Myśliwska 5
6.	GDDKiA Oddział w Kielcach	25-950 Kielce, ul. Paderewskiego 43/45
7.	GDDKiA Oddział w Krakowie	31-542 Kraków, ul. Mogilska 25
8.	GDDKiA Oddział w Lublinie	20-075 Lublin, ul. Ogrodowa 21
9.	GDDKiA Oddział w Łodzi	91-857 Łódź, ul. Irysowa 2
10.	GDDKiA Oddział w Olsztynie	10-083 Olsztyn, ul. Warszawska 89
11.	GDDKiA Oddział w Opolu	45-085 Opole, ul. Niedziałkowskiego 6
12.	GDDKiA Oddział w Poznaniu	60-673 Poznań, ul. Siemiradzkiego 5a
13.	GDDKiA Oddział w Rzeszowie	35-111 Rzeszów, ul. Legionów 20
14.	GDDKiA Oddział w Szczecinie	70-340 Szczecin, al. Bohaterów W-wy 33
15.	GDDKiA Oddział w Warszawie	03-808 Warszawa, ul. Mińska 25
16.	GDDKiA Oddział w Wrocławiu	54-155 Wrocław, ul. Lotnicza 24
17.	GDDKiA Oddział w Zielonej Górze	65-950 Zielona Góra, ul. Bohaterów Westerplatte 31

Załącznik nr 2 do Umowy

Wzór protokołu odbioru

Wykonawca:

Zamawiający:
Generalna Dyrekcja Dróg Krajowych i Autostrad, ul. Wronia 53, 00-874 Warszawa

Przedstawiciele Wykonawcy i Zamawiającego dokonali odbioru przedmiotu umowy Nr …… z dnia ……., stwierdzając komisyjnie, że:

1) ilość dostarczonych licencji jest zgodna z umową / nie jest zgodna z umową*)

2) ilość dostarczonych kompletów nośników z wersją instalacyjną oprogramowania jest zgodna z umową / nie jest zgodna z umową*)

3) ilość dostarczonych kluczy aktywacyjnych jest zgodna z umową / nie jest zgodna z umową*)

Nazwy i ilości każdej z dostarczonych licencji, nośników z wersją instalacyjną oprogramowania i kluczy instalacyjnych

1.

2.

Zgodnie z liczbą dostarczonych licencji

Odbiór ilościowy uznaje się za dokonany z wynikiem:

- pozytywnym *)

- negatywnym *)

Zastrzeżenia do odbioru - brak zgodności dostawy z umową polega na:

……

……

Protokół sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

....
(podpis przedstawiciela GDDKiA) (podpis przedstawiciela Wykonawcy)

<u>Zatwierdzam</u>:

.....
(podpis Dyrektora Departamentu Informacji i Informatyki GDDKiA)

*) niepotrzebne skreślić

ROZDZIAŁ IV

Formularz Oferty
i Formularze załączników do Oferty

(pieczęć Wykonawcy)	**OFERTA**

Generalna Dyrekcja Dróg Krajowych
i Autostrad ul. Wronia 53,
00-874 Warszawa

Nawiązując do ogłoszenia o postępowaniu o zamówienie publiczne prowadzonym w trybie przetargu nieograniczonego na dostawę dla GDDKIA nowych licencji, aktualizację już użytkowanych licencji oraz wsparcie techniczne i opiekę serwisową:

MY NIŻEJ PODPISANI

.....

.....

.....

działając w imieniu i na rzecz

.....

.....

.....

(nazwa (firma) dokładny adres Wykonawcy /Wykonawców)
(w przypadku składania oferty przez podmioty występujące wspólnie podać nazwy(firmy) i dokładne adresy wszystkich członków konsorcjum lub spółki cywilnej)

1. **SKŁADAMY OFERTĘ** na wykonanie przedmiotu zamówienia w zakresie określonym w Specyfikacji Istotnych Warunków Zamówienia.

2. **OŚWIADCZAMY,** że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia oraz wyjaśnieniami i zmianami SIWZ przekazanymi przez Zamawiającego i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.

3. **OFERUJEMY** wykonanie przedmiotu zamówienia za cenę:

…….…….. **zł brutto**

(*słownie złotych brutto: .....)*

OŚWIADCZAMY, że proponowana przez nas cena brutto zawiera 23% VAT.

4. **ZOBOWIĄZUJEMY SIĘ** do wykonania przedmiotu zamówienia w terminie wskazanym w SIWZ**.**

5. **AKCEPTUJEMY** warunki płatności określone przez Zamawiającego w Specyfikacji Istotnych Warunków Zamówienia.

6. **UWAŻAMY SIĘ** za związanych niniejszą ofertą przez czas wskazany w Specyfikacji Istotnych Warunków Zamówienia, tj. przez okres 60 dni od upływu terminu składania ofert.

7. **ZAMÓWIENIE ZREALIZUJEMY** sami*/przy udziale podwykonawców w następującym zakresie*

_____

(zakres powierzonych usług)

8. **OŚWIADCZAMY**, że sposób reprezentacji spółki* / konsorcjum* dla potrzeb niniejszego zamówienia jest następujący:

……
(Wypełniają jedynie przedsiębiorcy składający wspólną ofertę - spółki cywilne lub konsorcja)

9. **OŚWIADCZAMY,** że zapoznaliśmy się z postanowieniami umowy, określonymi w Specyfikacji Istotnych Warunków Zamówienia i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach określonych w Specyfikacji Istotnych Warunków Zamówienia, w miejscu i terminie wyznaczonym przez Zamawiającego.

10. **WSZELKĄ KORESPONDENCJĘ** w sprawie niniejszego postępowania należy kierować na poniższy adres:

_____

tel.: _____ faks : _____

11. **WADIUM** wnieśliśmy w dniu …….. w formie ……..

12. **OFERTĘ** niniejszą składamy na _____ stronach.

13. **WRAZ Z OFERTĄ** składamy następujące oświadczenia i dokumenty:

- _____
- _____

_____ dnia ___ ___ 2014 roku

_____

(podpis Wykonawcy/Pełnomocnika)

* niepotrzebne skreślić

Załącznik nr 1 do Formularza „Oferta”

(pieczęć Wykonawcy)	**OŚWIADCZENIE** **o spełnianiu warunków udziału w postępowaniu**

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego **na dostawę dla GDDKIA nowych licencji, aktualizację już użytkowanych licencji oraz wsparcie techniczne i opiekę serwisową**, na podstawie art. 44 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn.: Dz. U. z 2013 r. poz. 907 z późn. zm.; „ustawa Pzp”) oświadczamy, że spełniam(y) warunki udziału w wymienionym postępowaniu, stosownie do treści art. 22 ust. 1 ustawy Pzp.

_____ dnia ___ ___ 2014 roku

_____
(podpis Wykonawcy/Pełnomocnika)

Załącznik nr 2 do formularza „Oferta”

(pieczęć Wykonawcy)	**OŚWIADCZENIE** **o braku podstaw do wykluczenia**

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego **na dostawę dla GDDKIA nowych licencji, aktualizację już użytkowanych licencji oraz wsparcie techniczne i opiekę serwisową**, oświadczamy, że brak jest podstaw do wykluczenia mnie/nas z postępowania z powodu niespełnienia warunków określonych w art. 24 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn.: Dz. U. z 2013 r. poz. 907 z późn. zm.).

_____ dnia ___ ___ 2014 roku

_____
(podpis Wykonawcy/Pełnomocnika)

Załącznik nr 3 do formularza „OFERTA”

(pieczęć Wykonawcy)	**OŚWIADCZENIE** **o przynależności do grupy kapitałowej**

Składając ofertę w postępowaniu o zamówienie publiczne prowadzonym w trybie przetargu nieograniczonego **na dostawę dla GDDKIA nowych licencji, aktualizację już użytkowanych licencji oraz wsparcie techniczne i opiekę serwisową** oświadczamy, że:

*__nie należę__ do grupy kapitałowej, o której mowa w 24 ust. 2 pkt 5) ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn.: Dz. U. z 2013 r. poz. 907, z późn. zm.)

*__należę__ do tej samej grupy kapitałowej, o której mowa w 24 ust. 2 pkt 5) ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn.: Dz. U. z 2013 r. poz. 907, z późn. zm.), w skład której wchodzą następujące podmioty:

Lp.	Nazwa	Siedziba
1.		
2.		
(…)		

* niepotrzebne skreślić

_____ dnia ___ ___ 2014 roku

_____
(podpis Wykonawcy/Pełnomocnika)