OPIS PRZEDMIOTU ZAMÓWIENIA - SPECYFIKACJA TECHNICZNA

Część I: Systemu Elektronicznej Informacji Prawnej.

Przedmiotem zamówienia jest dostawa programu Systemu Elektronicznej Informacji Prawnej oraz 12 comiesięcznych aktualizacji, zgodnie z poniższym opisem:

Szczegółowy opis przedmiotu zamówienia: Systemu Elektronicznej Informacji Prawnej „LEX DLA SAMORZĄDU TERYTORIALNEGO"

Lp.	Nazwa	Ilość
1	Lex dla Samorządu Terytorialnego – wersja zabezpieczenia nolimit	1 szt.
2	Moduł Zamówienia Publiczne	1 szt.
3	Moduł Prawo Europejskie	1 szt.
4	Stanowisko mobilne do Lex ST nolimit	1 szt.
5	Stanowisko mobilne (on-line) do Lex ST nolimit	3 szt.

Zamawiający dopuszcza równoważny Systemu Elektronicznej Informacji Prawnej, spełniający następujące warunki równoważności:

Udzielenie przez Wykonawcę, Zamawiającemu licencji na korzystanie z programu System Elektronicznej Informacji Prawnej (SEIP) według konfiguracji:

a. Baza programu zainstalowana na serwerze wraz z nieograniczoną ilością stanowisk sieciowych podłączonych do bazy – (wersja sieciowa 1 szt.).
b. Baza programu zainstalowana na stacji roboczej – (wersja jednostanowiskowa 1 szt.),
c. Dostęp mobilny (on-line) dla terenowych jednostek organizacyjnych – (wersja mobilna 3 szt.).

Wymagania zawartości Systemu Elektronicznej Informacji Prawnej:

I. Bazę systemu muszą stanowić:

akty ze wszystkich dzienników urzędowych wymienionych w art. 8 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawych (t. j. Dz. U. z 2007 r., Nr 68, poz. 449).

II. Baza musi zawierać:

1. Dziennik Ustaw

a. Wszystkie akty obowiązujące oraz oczekujące.
b. Komplet tekstów aktów ujednoliconych i ocenionych, co do obowiązywania.
c. Wzajemne powiązania formalne między aktami (co najmniej relacje typu: zmienia - zmieniony przez, uchyla - uchylony przez, wykonuje - wykonywany przez, ujednolica - ujednolicony przez, wprowadza - wprowadzony przez, interpretuje - interpretowany przez).

d. Odwołania do przywołanych w aktach przepisów innych aktów prawnych, aktów wykonawczych; odwołanie do orzeczeń; odwołanie do pism urzędowych - z poziomu tekstu aktu.
e. Odwołania do cytatów/tez/pism z piśmiennictwa prawniczego; odwołania do komentarzy - z poziomu tekstu aktu prawnego z poziomu tekstu aktu prawnego.

2. Monitor Polski

a. Komplet informacji formalnych o aktach(co najmniej: identyfikator, tytuł, organ wydający, data uchwalenia lub wydania aktu, data ogłoszenia, data wejścia w życie, data utraty mocy).
b. Wszystkie akty obowiązujące oraz oczekujące.
c. Komplet tekstów aktów ujednoliconych i ocenionych, co do obowiązywania.

3. Dzienniki Urzędowe

Ujednolicone teksty aktów prawnych opublikowanych w Dziennikach Urzędowych naczelnych i centralnych organów administracji rządowej, w tym:

4. Dziennik Urzędowy Unii Europejskiej seria L - wydanie polskie

a. Komplet informacji formalnych o aktach opublikowanych w tym dzienniku. (co najmniej: identyfikator, tytuł, organ wydający, data uchwalenia lub wydania aktu, data ogłoszenia, data wejścia w życie).
b. Komplet tekstów aktów ujednoliconych i ocenionych, co do obowiązywania, opublikowanych w tym dzienniku.
c. Wzajemne powiązania formalne między aktami (co najmniej relacje typu: zmienia - zmieniany przez, uchyla - uchylony przez, wykonuje - wykonywany przez).
d. Odwołania do przywołanych w aktach przepisów innych aktów prawnych, aktów wykonawczych; odwołania do orzeczeń - z poziomu tekstu aktu.

5. Dziennik Urzędowy Unii Europejskie seria C - wydanie polskie

a. Komplet informacji formalnych o aktach opublikowanych w tym dzienniku. (co najmniej: identyfikator, tytuł, organ wydający, data uchwalenia lub wydania aktu, data ogłoszenia, data wejścia w życie).
b. Wzajemne powiązania formalne między aktami (co najmniej relacje typu: zmienia - zmieniany przez, uchyla - uchylony przez, wykonuje - wykonywany przez).

6. Dzienniki Urzędowe Unii Europejskiej - polskie wydanie specjalne

a. Komplet informacji formalnych o aktach opublikowanych w tym dzienniku (co najmniej: identyfikator, tytuł, organ wydający, data uchwalenia lub wydania aktu, data ogłoszenia, data wejścia w życie).
b. Wszystkie akty obowiązujące oraz oczekujące.
c. Komplet tekstów aktów ujednoliconych i ocenionych, co do obowiązywania, opublikowanych w tym dzienniku.
d. Wzajemne powiązania formalne między aktami (co najmniej relacje typu: zmienia - zmieniony przez, uchyla - uchylony przez, wykonuje - wykonywany przez).
e. Odwołania do orzeczeń z poziomu tekstu aktu.

III. Ponadto, baza systemu musi zawierać:

1. Komplet tekstów aktów prawnych opublikowanych w wojewódzkich dziennikach urzędowych od wprowadzenia 16 województw ustawą z dnia 24 lipca 1998 r. o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa.
   a. Akty prawa powinny być objęte klasyfikacją przedmiotową.
   b. Teksty aktów powinny podlegać ujednoliceniu i być prezentowane w wersjach czasowych.
   c. Metryki aktów powinny zawierać informację o relacjach między aktami.
2. Wzory pism i umów, w tym zbiór obowiązujących formularzy urzędowych opublikowanych w Dziennikach Ustaw i Monitorach Polskich.
3. Orzeczenia Sądu Najwyższego, Naczelnego Sądu Administracyjnego, Wojewódzkich Sądów Administracyjnych, Trybunału Konstytucyjnego oraz sądów apelacyjnych.
4. Niepublikowane orzeczenia SN, NSA i WSA.
5. Orzeczenia administracyjne w tym m.in. Głównej Komisji Orzekającej w Sprawach o Naruszenie Dyscypliny Finansów Publicznych przy Ministerstwie Finansów.
6. Orzeczenia Zespołu Arbitrów/Krajowej Izby Odwoławczej przy Prezesie Urzędu Zamówień Publicznych.
7. Orzeczenia Europejskiego Trybunału Sprawiedliwości i Sądu Pierwszej Instancji.
8. Projekty ustaw wraz z uzasadnieniami.
9. Komentarze (w tym skomentowana część jednostek redakcyjnych: Kp, Kpa, KRO, Kc, Kpc, Kpk) monografie i inne opracowania dotyczące prawa polskiego i europejskiego.
10. Bibliografia prawnicza.
11. Baza adresowa sądów, urzędów centralnych oraz prokuratur.
12. Uzasadnienia do orzeczeń opublikowanych w zbiorach urzędowych.
13. Cytaty/Tezy/Pisma z piśmiennictwa prawniczego.

IV. Wymagania dotyczące funkcjonalności systemu informacji prawnej.

1. Sposoby wyszukiwania.

a. Wyszukiwania wg identyfikatora / sygnatury.
b. Wyszukiwania wg rocznika.
c. Wyszukiwania wg daty wydania/opublikowania/obowiązywania.
d. Wyszukiwanie poprzez klasyfikację przedmiotową (dotyczy bazy aktów prawnych i orzeczeń).
e. Wyszukiwanie wg słów w treści dokumentów.
f. Wyszukiwanie wg numeru: KRS - dla MSiG, PKD - dla MP B.
g. Wyszukiwanie po nazwie podmiotu w MSiG, MP B, MS B.
h. Wyszukiwanie po siedzibie podmiotu w Mig.

2. Wymagania dodatkowe.

a. Pisma urzędowe naczelnych i centralnych organów administracji rządowej oraz agencji rządowych i innych instytucji państwowych (obecne i archiwalne).
b. Możliwość porównania treści przepisu aktu prawnego w brzmieniu przed zmiana treści przepisu - po zmianie.

c. Możliwość dokonywania przez użytkownika zmiany daty oceny, co do obowiązywania aktów z Dz. U. i M.P., czego efektem ma być przywołanie całego systemu prawa - aktów obowiązujących, nieobowiązujących oraz oczekujących (wersji tekstów oraz relacji między aktami) na dowolnie wpisany dzień z przeszłości.
d. Wyodrębnienie w zakresie Dz. U. i M.P. osobnych baz z aktami: obowiązującymi, nieobowiązującymi (archiwalnymi) i oczekującymi.
e. Oznaczenie identyfikacji aktów obowiązujących, nieobowiązujących i oczekujących publikowanych w Dz. U. i M. P.
f. Możliwość kopiowania całości lub części dokumentów bezpośrednio z systemu do edytorów tekstów.
g. Możliwość wydruku z systemu w sposób poprawny (w formacie wyświetlonym na monitorze): całego aktu, jednostek redakcyjnych, zaznaczonego fragmentu, z przypisami i bez przypisów.
h. Możliwość wyświetlenia treści całego aktu prawnego.
i. Dostęp do czasopism dedykowanych samorządowi terytorialnemu.

V. Wymagania techniczne systemu elektronicznej informacji prawnej.

a. System musi zapewnić pełną, opisaną powyżej, funkcjonalność, dla stanowisk sieciowych podłączonych do serwera, przy braku dostępu do Internetu.
b. Oprogramowanie musi poprawnie działać na autonomicznych stacjach roboczych i stacjach podłączonych do serwerów sieci LAN i WAN z zainstalowanym tym oprogramowaniem.
c. Możliwość instalacji na serwerach i stacjach roboczych działających pod kontrolą systemu operacyjnego Microsoft Windows 2003 oraz nowszych.
d. Program musi posiadać zabezpieczenia przed nieautoryzowanym dostępem.
e. Poprawność wydruków z programu na drukarkach sieciowych i autonomicznych.
f. Program powinien umożliwiać pracę on-line ze stale aktualizowaną oraz ujednoliconą bazą danych w systemie codziennym.

Część II: Oprogramowanie zabezpieczające.

Przedmiotem zamówienia jest dostawa oprogramowania zabezpieczającego, zgodnie z poniższym opisem:

Szczegółowy opis przedmiotu zamówienia: System antywirusowy.

Lp.	Nazwa	Ilość
1	Odnowienie posiadanych licencji Symantec Multi-Tier Protection 11.0.2 Basic GOV	160 szt.
2	Zakup licencji Symantec Multi-tier Protection 11.0.2 Basic GOV	50 szt.

Szczegółowy opis przedmiotu zamówienia: Centralny system backup i archiwizacji.

Lp.	Nazwa	Ilość
1	SYMANTEC BACKUP EXEC SERVER 12.5 WIN PER SERVER BNDL PROMO COMP UG LIC EXPRESS BAND S BASIC 12MO	5 szt.
2	SYMANTEC BACKUP EXEC AGENT FOR MSFT EXCHANGE 12.5 WIN PER SERVER BNDL STD LIC GOV BAND S BASIC 12MO	1 szt.
3	SYMANTEC BACKUP EXEC AGENT FOR MSFT SQL 12.5 WIN PER SERVER BNDL STD LIC GOV BAND S BASIC 12MO	2 szt.
4	SYMANTEC BACKUP EXEC OPTION CENTRAL ADMIN SERVER 12.5 WIN PER SERVER BNDL STD LIC GOV BAND S BASIC 12MO	1 szt.

Zamawiający dopuszcza równoważny system backup i archiwizacji, spełniający następujące warunki równoważności:

Cały system umożliwiać musi zabezpieczenie serwerów wymienionych w tabeli nr 1:

Lp	Nazwa	Model	System Operacyjny	Ilość procesorów	Rola	Baza danych	Przewidywany sposób zabezpieczenia
1	Serwer1	Dell PowerEdge T610	Windows 2008 x64 ENG	2	Główny Kontroler domeny (PDC, RID)		Full backup, Disaster recovery
2	Serwer2	Dell PowerEdge T610	Windows Serv 2008 x64 ENG	2	Zapasowy kontroler domeny, Domain naming, Schema master	SQL 2005	Full backup
3	Serwer3	Dell PowerEdge 2950	Windows 2008 x64 ENG	2	Serwer Exchange		Full backup
4	Serwer4	HP Prowiant ML370	Windows 2003	2	Aplikacje	SQL 2005	Full backup
5	Serwer5	Dell PowerEdge R300	Windows 2003	2	ISA Server		Full backup

Tabela nr 1: Systemy zabezpieczenia przed utrata danych - minimalne wymagania zamawiającego dotyczące sposobu zabezpieczenia

I. Wymagania ogólne:

1. System powinien być przeznaczony dla średnich i dużych firm, które mają rozbudowane środowisko informatyczne, powinien oferować elastyczną architekturę (serwer zarządzający/media-serwer/klient) celem sprostania rozwojowi środowiska informatycznego.
2. System musi cechować bardzo efektywne wykorzystanie napędów taśmowych, tzn. system musi być zoptymalizowany do użycia jak najmniejszej ilości napędów taśmowych.
3. System musi zapisywać dane na taśmach tak zoptymalizowane, aby nie było potrzeby wykonywania żadnych dodatkowych działań (nawet automatycznych) celem ich optymalizacji.
4. Powinien umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej.
5. Brak preferowanego dostawcy hardware dla którego dostępna jest bogatsza funkcjonalność (macierze, biblioteki taśmowe…), musi istnieć możliwość zmiany producenta sprzętu bez utraty funkcjonalności backupu.
6. Powinien być łatwy w instalacji, konfigurowaniu i zarządzaniu poprzez interfejs graficzny (GUI). Powinien umożliwiać pełne dostosowanie do środowiska klienta.
7. Powinien posiadać funkcje monitoringu, generator raportów.
8. Powinien umożliwiać backup po sieci LAN i SAN serwerów z Windows 2003/2008.
9. Do przechowywania danych wykorzystywane powinny być bezobsługowe biblioteki taśmowe bądź lokalne dyski.
10. Możliwość stosowania go w środowisku Storage Area Network, co zapewni dużą szybkość wykonywanych backupów oraz współdzielenie napędów taśmowych pomiędzy serwery backupowe w sieci SAN.
11. Powinien posiadać możliwość równoczesnego zapisu/ odczytu na wielu napędach taśmowych w tym samym czasie.
12. Powinien potrafić backupować online bazy danych, np. Oracle, Exchange, SQL Server, DB2.
13. Backup i odtwarzanie serwera Exchange powinno umożliwiać odtworzenie na poziomie pojedynczej wiadomości w skrzynkach użytkowników. Opcja powinna umożliwiać odzyskiwanie z backupu bazy danych bez dodatkowego backupu skrzynek pocztowych w trybie MAPI.
14. Powinien posiadać również wbudowany mechanizm do backupowania otwartych plików.
15. Powinien potrafić wykorzystywać do backupu mechanizm kopii migawkowych systemu Microsoft Windows 2003 (VSS).
16. Oferować możliwość rozszerzenia o funkcję disaster–recovery dla systemu Windows umożliwiające proste i szybkie automatyczne odtworzenie serwera po awarii zapewniające integralność i spójność danych, opcja ta powinna być integralną częścią systemu backupowego.
17. Automatyczny backup bazujący na kalendarzu. Możliwość backupu typu: full, incremental, differential.

18. Musi umożliwiać wykonywania skryptów przed i po backupie (np. uruchamianych przed backupem bazy oraz po wykonaniu backupu off-line bazy, kasowanie redo logów).
19. Możliwość szyfrowania danych przesyłanych przez sieć LAN. Opcja powinna być ściśle zintegrowana z produktem do backupu.
20. Możliwość kompresji na kliencie backupowym przed wysłaniem danych przez sieć.
21. Wymagana jest możliwość pracy w klastrze serwerów z Microsoft Windows również Windows 2008.
22. Posiadać możliwość wykonywania backupów na urządzenia dyskowe, które następnie będą automatycznie powielane na nośniki taśmowe (D2D2T). System backupowy powinien, tak długo jak dane obecne są na dyskach, wykorzystywać je w procesach restore, znacznie skracając czas odtworzenia danych.
23. Oprogramowanie powinno oferować funkcjonalność pozwalającą zminimalizować ilość koniecznych do wykonywania powtarzalnych pełnych kopii danych systemów plików.
24. Serwery backupowe powinny móc zapisywać dane na te same napędy taśmowe poprzez sieć SAN, zastosowanie urządzeń z NDMP musi umożliwiać backup na te same napędy taśmowe.
25. Opcjonalnie system powinien umożliwiać backup na poziomie plików dla stacji klienckich i komputerów przenośnych, oprogramowanie powinno cechować się możliwością pracy online i offline, gdzie przy pracy offline po wykonaniu kopii danych, są one backupowane w momencie podłączenia do sieci. Oprogramowanie powinno posiadać funkcjonalność umożliwiającą backup przyrostowy plików pst.
26. System powinien mieć możliwość monitowania i alterowania poprzez email i SNMP.
27. Powinien posiadać możliwość backupu online danych z systemu SharePoint Portal Server, wraz z odtwarzanie pojedynczych dokumentów z jednoprzebiegowego backupu.
28. Musi mieć możliwość zintegrowania się z technologią VCB (Vmware Consolidate Backup) celem wydajnego backupu danych z możliwością odtwarzania pojedynczych plików (zawartych w VMDK dla systemów Windows), backup musi być wykonywany jednoprzebiegowo (cały plik VMDK backupowany raz).
29. Musi wspierać dla technologii wirtualizacyjnych firmy Microsoft (Hyper-V), z możliwością odtwarzania pojedynczych plików z maszyn wirtualnych Windows z jednoprzebiegowego backupu.
30. System musi (jako opcja) oferować ciągłą ochronę (continuous protection).
31. System powinien posiadać (jako opcja) możliwość wykonania backupu Active Directory a następnie odzyskania pojedynczych obiektów AD bez restartu i resynchronizacji systemu. Backup ten powinien być wykonywany jednoprzebiegowo.
32. System musi mieć możliwość centralnego zarządzania serwerami (Media Serwerami) systemu backupowego.
33. Możliwość backupu poprzez sieć SAN zasobów z serwerów Linux.
34. Pełne wsparcie dla backupu online MS SQL 2005 oraz nowszych.
35. Możliwość współpracy z MOM (Microsoft Operations Manager 2005).
36. Musi posiadać (jako opcja) możliwość backupu stacji roboczych Windows, z funkcjonalnościami umożliwiającymi optymalizację transferu danych poprzez łącza WAN, wykonywania zadań backupowych nawet wtedy gdy stacja nie jest podłączona do sieci (backup poprzez bufor i synchronizacja po ustanowieniu połączenia), oraz

mechanizm backupowania plików pst (MS Outlook) tak by transferować tylko zmiany w tych plikach a nie za każdym razem całe pliki.

37. Musi posiadać (jako opcja) moduł bazodanowy do backupu systemu Symantec Enterprise Vault.

Część III: System wspierający modelowanie systemów ISO oraz zarządzanie organizacją.

Przedmiotem zamówienia jest dostawa oprogramowania wspierającego modelowanie systemów ISO oraz zarządzanie organizacją, zgodnie z poniższym opisem:

Szczegółowy opis przedmiotu zamówienia: Oprogramowanie Smart, w którego skład wchodzą moduły: Smart Architekt, Smart Portal, Smart Audyt, Smart Reports oraz oprogramowanie zarządzania ryzykiem Risk Manager.

Zamawiający dopuszcza równoważne oprogramowanie wspierającego modelowanie systemów ISO zarządzanie organizacją, spełniające następujące warunki równoważności:

1. Autoryzowany dostęp do poszczególnych procesów - zabezpieczanie przed nieuprawnionymi modyfikacjami.
2. Możliwość tworzenia wielu poziomów procesów - od procesów głównych poprzez podprocesy aż do pojedynczych działań i czynności.
3. Możliwość definiowania informacji o procesach takich jak: dane wejściowe i wyjściowe, właściwości procesu, uczestników, dokumenty i formularze itd.
4. Możliwość definiowania i prezentacji wskaźników i mierników procesów.
5. Rozbudowany edytor graficzny pozwalający na rozrysowanie procesu wg wcześniej obranych założeń.
6. Możliwość rysowania schematów graficznych w narzędziu do tego dedykowanym.
7. Tworzenie dowolnej bazy atrybutów, atrybuty mogą mieć charakter; daty, wartości, łącza do elementu projektu(linku), linku do strony www, opisu.
8. System musi automatycznie rejestrować zmiany merytoryczne i pozwalać na ich późniejsze analizowanie. Użytkownik może w dowolnym momencie przeglądać archiwum.
9. Automatyczna zmiana nazw, wartości atrybutów w całej bazie w przypadku zmiany wartości dla dowolnego elementu posiadającego kilka wystąpień.
10. Możliwość dowolnego modelowania struktury - oddzielne lub połączone wskazanie poszczególnych grup elementów (dokumenty, procesy, audyty, raporty).
11. Automatyczne generowanie karty zmian.
12. Możliwość wysyłania wiadomości pomiędzy użytkownikami.
13. Możliwość tworzenia grup użytkowników.
14. Możliwość symultanicznego tworzenia map procesów przez rozproszony przestrzennie zespół zadaniowy.
15. Możliwość zdalnej pracy wielu użytkowników - rysowanie map procesów przez właścicieli/liderów procesów przy jednoczesnej zdalnej pracy z konsultantem lub liderem projektu.
16. Możliwość sprawnego zaplanowania i przeprowadzenia auditów - automatyczne powstawanie harmonogramu auditów.
17. Możliwość planowania auditów z wykorzystaniem bazy wiedzy powstałej podczas przeprowadzania auditów wcześniejszych (cel, obszar, pytania, niezgodności, skuteczność działań).
18. Autoryzowany dostęp użytkowników do procesu auditu w ramach przydzielonych uprawnień.

19. Możliwość korzystania z list wyboru: auditorów wewnętrznych, auditowanych celów, pytań auditowych itd. przy planowaniu auditów.
20. Możliwość tworzenia listy pytań na podstawie wskazanego obszaru auditowania wg procesu, komórki organizacyjnej lub innego zdefiniowanego zakresu.
21. Możliwość przeprowadzenia auditu, odnotowywanie odpowiedzi, dowodów i wniosków z auditu w formie elektronicznej.
22. Możliwość załączania dowodów do procesu auditu w formie dowolnych plików.
23. Możliwość zamknięcia audytu – zabezpieczenia przed nieuprawnionymi zmianami.
24. Możliwość skorzystania z kreatora raportów umożliwiającego użytkownikowi samodzielne tworzenie rejestrów i raportów oraz przeprowadzenie analizy z wyników przeprowadzonych auditów
25. Dane ze wszystkich auditów gromadzone w jednej, centralnej bazie danych.
26. Możliwość bezpośredniego przekazywania informacji i danych o audicie do aplikacji z dowolnego komputera w sieci wewnętrznej lub zewnętrznej.
27. Możliwość definiowania różnych typów niezgodności i przypisywania im odpowiednich ścieżek obiegu.
28. Etapowa realizacja działań korekcyjnych, korygujących lub zapobiegawczych poprzez wyznaczone osoby w określonym czasie.
29. Możliwość automatycznego generowania monitów przypominających pracownikom o realizacji poszczególnych etapów działań.
30. Możliwość kontaktu audytowany (odpowiedzialny za usunięcie np. niezgodności) – z audytującym on-line.
31. Możliwość automatycznego generowania i aktualizacji rejestrów oraz raportów związanych z niezgodnościami oraz podjętymi działaniami.
32. Możliwość definiowania i edycji podstawowych parametrów funkcji ryzyka.
33. Możliwe tworzenie i modyfikacja list: ryzyk, aktywów mających ściśle określoną wartość dla danego przedsiębiorstwa, zagrożeń, podatności.
34. Możliwość definiowania i modyfikacji skali wartości dla poszczególnych aktywów, zagrożeń i podatności.
35. Możliwość dokonywania cyklicznej realizacji procesu szacowania ryzyka w oparciu o utworzoną wcześniej bazę wiedzy.
36. Możliwość tworzenie bazy użytkowników którzy będą brali udział w procesie szacowania ryzyka, w ramach przydzielonych im uprawnień.
37. Możliwość podglądu wyników pracy związanej z zarządzaniem ryzykiem użytkowników posiadających do tego uprawnienia.
38. Możliwość eksportu danych z aplikacji do plików zewnętrznych.
39. Możliwość tworzenia centralnej bazy danych zawierającej np. wszystkie aktywa lub też przypuszczalne zagrożenia i autoryzowany dostęp do tych danych.
40. Możliwość automatycznego otrzymywania, przez osoby uprawnione, pełnych analiz związanych z procesem szacowania ryzyka w organizacji.
41. Dostęp osób uprawnionych do pełnej historii szacowania ryzykiem.
42. Konfiguracja kategorii ryzyka.
43. Konfiguracja przyczyn wystąpienia ryzyka.
44. Tworzenie struktury organizacyjnej według stanowisk i departamentów.
45. Tworzenie struktury organizacyjnej według lokalizacji.
46. Identyfikacja ryzyka na podstawie procesów.
47. Identyfikacja ryzyka w odniesieniu do celów organizacji.
48. Wyznaczanie właścicieli ryzyka.

49. Wyznaczanie częstotliwości dokonywania ocen ryzyka.
50. Ocena ryzyka wedle skutku i prawdopodobieństwa jego realizacji.
51. Ocena różnego rodzaju skutków.
52. Ocena kwotowa skutku realizacji ryzyka.
53. Ocena poziomu ryzyka inherentnego, rezydualnego i oczekiwanego.
54. Wyszukiwanie ryzyk z wykorzystaniem rozbudowanego filtra.
55. Konfiguracja macierzy ryzyka.
56. Wyznaczanie właścicieli reakcji na ryzyko.
57. Monitorowanie stopnia realizacji reakcji na ryzyko.
58. Identyfikacja zabezpieczeń.
59. Przypisanie właścicieli zabezpieczeń.
60. Baza zabezpieczeń.
61. Wyszukiwanie zabezpieczeń z wykorzystaniem filtra.
62. Generowanie raportów z listy dostępnych szablonów.
63. Filtrowanie danych na potrzeby raportów.
64. Zapis w formacie np. PDF, HTML, XLS, RTF.
65. Nadawanie uprawnień użytkownikom.
66. Tworzenie kategorii uprawnień dla użytkowników.
67. Nadawanie dostępu do poszczególnych ryzyk.
68. Możliwość rejestrowania dokumentów przez uprawnione do tego osoby.
69. Możliwość definiowania praw dostępu do dokumentów na różnych poziomach (przegląd, opiniowanie, zatwierdzanie, modyfikacja).
70. Możliwość automatycznego generowania i wysyłania drogą e-mail oraz w tablicy informacyjnej, monitów przypominających pracownikom o wykonaniu czynności związanych z dokumentem np. monity o przegląd, opiniowanie czy zatwierdzenie.
71. Możliwość automatycznej dystrybucji dokumentu na podstawie przydzielonych uprawnień.
72. Kontrola nad wersjami dokumentacji – w przypadku obowiązywania nowej wersji dokumentu stara nieaktualna wersja automatycznie przechodzi do archiwum.
73. Automatycznie generowana karta zmian.
74. Dziennik zdarzeń każdego dokumentu – np. informacja kto i kiedy zapoznał się z danym dokumentem.
75. Możliwość skorzystania z kreatora raportów umożliwiającego użytkownikowi samodzielne i wykonywanie rejestrów i raportów związanych z przechowywanymi w bazie dokumentami.
76. Możliwość importu gotowych dokumentów (np: doc, PDF, xls, bmp, avi, inne) lub tworzenia nowych.
77. Możliwość zgłaszania potrzeby opracowania nowego dokumentu lub propozycji zmian w dokumencie istniejącym.
78. Możliwość generowania raportów z listy dostępnych szablonów.
79. Filtrowanie danych na potrzeby raportów.
80. Tworzenie raportów pozwalających na graficzną prezentację zgromadzonych danych.
81. Zapis w formacie np. RPT, HTML, XLS, RTF, TTX, TXT, XML, BMP, JPEG, TIFF, GIF, CSV, e-mail.
82. Możliwość tworzenia pełnej struktury organizacyjnej, na różnych poziomach szczegółowości – od struktury ogólnej do szczegółowego widoku.
83. Możliwość tworzenia struktury odpowiedzialności w zależności od pełnionych ról, przynależności do grup, itp.

84. Możliwe automatyczne generowanie uprawnień, w oparciu o strukturę organizacyjną / odpowiedzialności i zajmowane miejsce w organizacji.
85. Dowolne przypisywanie atrybutów do definicji struktury organizacyjnej / odpowiedzialności(np. adresy e-mail, nr telefonów, informacje o zakresach obowiązków, wymaganych kompetencjach).
86. Możliwość generowania raportów w oparciu o strukturę organizacyjną.
87. Możliwość automatycznego definiowania użytkowników na podstawie struktury organizacyjnej lub Active Directory.

System musi posiadać portal pracowniczy umożliwiający:

1. System nadawania uprawnień dostępu do danych.
2. Możliwość integracji dostępu z domeną.
3. Wizualizację diagramów procesów.
4. Podgląd do wcześniej zdefiniowanych atrybutów.
5. Podgląd do statusu zgłoszonych zmian (zaakceptowane, odrzucone).
6. Powiadamianie o zmianach.
7. Podgląd na historię zmiany.
8. Możliwość dodawania elementów do grupy ulubionych.
9. System zakładkowy – możliwość otwarcia (przeglądania) kilku diagramów / dokumentów jednocześnie.
10. Przeglądanie elementów – według drzewa projektu lub listy elementów.
11. Przejrzysty podział elementów – procesy/dokumenty, polityki/ryzyka/audyty.
12. Możliwość przeglądania diagramów według określonych elementów czynności/dokumentów/odpowiedzialności – automatyczne wskazywanie danego elementu.
13. Wyszukiwarka danych – dostęp do pożądanego elementu (dokumentu, diagramu, stanowiska, czynności, itp.).

Część IV: Dostawa licencji i oprogramowania.

Przedmiotem zamówienia jest dostawa Licencji.

Szczegółowy opis przedmiotu zamówienia: Licencje.

Lp.	Nazwa	Ilość
1	Licencja dostępowa Exchange Server 2007 MOLP GOV	40 szt.
2	Microsoft Windows 7 Ultimate PL BOX	3 szt.
3	Adobe CS4 Web Premium IE Win	1 szt.