Załącznik nr 1 do SWZ
Znak sprawy: GK.271.2.2026.MG

Szczegółowy opis przedmiotu zamówienia

dla zamówienia pn.:

„Dostawa i wdrożenie Teleinformatycznego Systemu Zarządzenia Bezpieczeństwem Informacji”

w ramach projektu ”Podniesienie poziomu ochrony cybernetycznej w gminie Unisław, poprzez realizację zaplanowanych działań w obszarach organizacyjnym, kompetencyjnym oraz technicznym” realizowanego w ramach projektu Cyberbezpieczny Samorząd” dofinansowanego w formie grantu
z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)
Priorytet II: Zaawansowane usługi cyfrowe,
Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Opracował:

Mariusz Bartosik

Unisław, luty 2026 r.

1. Przedmiot zamówienia.

Przedmiotem zamówienia jest kompleksowa realizacja przedsięwzięcia polegającego na dostarczeniu, instalacji, konfiguracji, integracji, uruchomieniu oraz wdrożeniu Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji w środowisku teleinformatycznym Zamawiającego.

2. Zakres zamówienia.

- Dostarczenie, instalację i konfigurację systemu,
- Parametryzację zgodnie z wymaganiami Zamawiającego,
- Integrację z systemami Zamawiającego oraz systemami zewnętrznymi, w tym administracji publicznej,
- Wykonanie testów funkcjonalnych, technicznych i integracyjnych,
- Uruchomienie systemu w środowisku produkcyjnym,
- Przeprowadzenie szkoleń dla administratorów i użytkowników,
- Zapewnienie gwarancji oraz wsparcia technicznego.

3. Opis systemu.

Teleinformatyczny System Zarządzania Bezpieczeństwem Informacji

DEFINICJE

Administrator systemu – osoba odpowiedzialna za merytoryczne funkcjonowanie wdrażanych rozwiązań z ramienia Zamawiającego.

Aplikacja mobilna - Aplikacja mobilna dostępna na urządzania mobilne, dająca dostęp do części funkcjonalności
Systemu.

Aktualizacja Systemu – uaktualnienia, wersje zmodyfikowane lub rozszerzone, dodatki.

API – Application Programming Interface, interfejs programowania aplikacji – jest to sposób rozumiany jako ściśle określony zestaw reguł i ich opisów, w jaki programy komunikują się między sobą. API definiuje się na poziomie kodu źródłowego dla takich składników oprogramowania jak np. aplikacje, biblioteki czy system operacyjny. Zadaniem API jest dostarczenie odpowiednich specyfikacji podprogramów, struktur danych, klas obiektów i wymaganych protokołów komunikacyjnych. Elementem API jest dokumentacja techniczna umożliwiająca jego wykorzystanie przez zewnętrzne systemy.

BIP – strona podmiotowa Biuletynu Informacji Publicznej.

CRWDE – Centralne Repozytorium Wzorów Dokumentów Elektronicznych.

CMS – system zarządzania treścią – oprogramowanie pozwalające na łatwe tworzenie i prowadzenie serwisu WWW, również przez redakcyjny personel nietechniczny.

Dane Osobowe – informacje dotyczące osoby w rozumieniu ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tj.. Dz.U. 2019 poz. 1781)oraz norm prawnych wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich

danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r., Nr 119, poz. 1).
Dokument Elektroniczny – Dokument Elektroniczny w rozumieniu przepisów art. 3 ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj.. Dz.U. z 2024 poz. 307)
ePUAP – Elektroniczna Platforma Usług Administracji Publicznej https://epuap.gov.pl.
ESP – Elektroniczna Skrzynka Podawcza.
EZD – Elektroniczne Zarządzanie Dokumentacją, oprogramowanie umożliwiające wykonywanie czynności kancelaryjnych w podmiocie oraz postępowanie z dokumentacją począwszy od wpływu lub powstania dokumentacji wewnątrz podmiotu, poprzez dokumentowanie przebiegu załatwiania i rozstrzygania spraw, aż do momentu uznania dokumentacji za część dokumentacji w archiwum zakładowym i jej obsługi w ramach archiwum zakładowego zgodnie z wymaganiami Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r., w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, Dz. U. 2011 nr 14 poz. 67).
Formularz Elektroniczny – Graficzny interfejs użytkownika wystawiany przez oprogramowanie służący do przygotowania wygenerowania dokumentu elektronicznego zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego w rozumieniu przepisów rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 roku w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2018, poz. 180, tj..).
Konto Firmowe (KF) – Konto podmiotu niebędącego osobą fizyczną - sp. z o.o., S.A., sp. komandytowa, fundacja, stowarzyszenie oraz inne.
Krajowy Węzeł Tożsamości (KWT) – rozwiązanie umożliwiające uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego.
Instrukcja obsługi – dokument zawierający zasady działania i obsługi Systemu.
Kopia bezpieczeństwa systemu (BACKUP) – dane i pliki, które mają służyć do odtworzenia oryginalnych danych
w przypadku ich utraty lub uszkodzenia.
Korzystanie – uzyskiwanie dostępu i używanie funkcjonalności Systemu.
Licencja – uprawnienie udzielane przez Wykonawcę Zamawiającemu uprawniające do Korzystania z Systemu.
Naprawa – oznacza przywrócenie funkcjonowania Systemu poprzez usunięcie Błędu (błędu krytycznego, błędu, usterki) i doprowadzenie Systemu do działania zgodnego ze sposobem funkcjonowania opisanym w instrukcji obsługi Systemu.
Obejście – oznacza przywrócenie funkcjonowania Systemu poprzez zminimalizowanie uciążliwości Błędu (błędu krytycznego, błędu, usterki). Obejście nie stanowi naprawy, jednak pozwala korzystać nieprzerwanie z wszystkich funkcjonalności Systemu e-Urząd.
Portal – System dostępny za pośrednictwem przeglądarki internetowej.
Profil Zaufany (PZ) – zestaw informacji identyfikujących i opisujących podmiot lub

osobę będącą użytkownikiem konta na ePUAP, który został w wiarygodny sposób potwierdzony przez organ podmiotu określonego w art. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj.. Dz.U. 2024 poz. 307).

Podpis Zaufany – podpis elektroniczny, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji. Podpis Zaufany zawiera dane identyfikujące osobę (imię, nazwisko oraz numer PESEL), ustalone na podstawie środka identyfikacji elektronicznej wydanego w systemie, o którym mowa w art. 20aa pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, identyfikator środka identyfikacji elektronicznej, przy użyciu którego został złożony oraz czas jego złożenia.

Protokół Odbioru – dokument potwierdzający wykonanie i zakończenie wdrożenia przedmiotu Umowy.

PUSH – powiadomienie wyświetlane na urządzeniu mobilnym.

Specyfikacja techniczno-funkcjonalna – dokument ustalający wymagania techniczne oraz funkcjonalne, które powinien spełniać System.

System – pojęcie obejmujące Elektroniczne Biuro Obsługi Interesanta, Systemy Dziedzinowe oraz BIP.

System e-Urząd – rozwiązanie informatyczno-funkcjonalne dostępne za pośrednictwem przeglądarki internetowej lub aplikacji mobilnej, za pomocą którego Użytkownik otrzymuje między innymi dostęp do swoich danych podatkowych i księgowych zgromadzonych w systemach informatycznych danego urzędu, możliwość wysłania dokumentów elektronicznych skierowanych do urzędu, opłacenia zobowiązania, umówienia wizyty w urzędzie oraz za pomocą którego ma możliwość otrzymania powiadomień o najważniejszych wydarzeniach lokalnych.

System Dziedzinowy (SD) – zintegrowany system informatyczny dedykowany do obsługi działalności Urzędu do realizacji zadań związanych z prowadzenia rejestru mieszkańców, prowadzenia rejestru wyborców, pobierania danych z SRP, naliczania podatków rolnego, leśnego i od nieruchomości, naliczania podatku od środków transportowych, windykacji wszystkich naliczonych podatków i opłat, gospodarowania odpadami komunalnymi, fakturowania, rejestracji wpłat gotówkowych i bezgotówkowych, prowadzenia rejestru umów, zaangażowania i zobowiązań, prowadzenia kadr i płac oraz udostępniania niezbędnych danych pracownikom a także centralnego nadawania uprawnień oraz kontroli poprawności oraz wymiany danych pomiędzy poszczególnymi modułami, z którego m. in. są wizualizowane dane Użytkowników.

System Transakcyjny – Usługa dostępna w Internecie umożliwiająca wykonanie płatności.

UKF – Upoważnienie do Konta Firmowego.

UPD – Urzędowe Poświadczenie Dostarczenia.

UPO – Urzędowe Poświadczenie Odbioru.

UPP – Urzędowe Poświadczenie Przedłożenia.

Użytkownik– osoba fizyczna lub osoba prawna, którym Urząd udostępnia System celem Korzystania w zakresie określonym przez Wykonawcę i Użytkownika końcowego Systemu; Użytkownik końcowy Systemu nie posiada sublicencji do Systemu i nie jest uprawniony do dalszego udostępniania Systemu.

VPN- Virtual Private Network, wirtualna sieć prywatna – tunel, przez który płynie

ruch w ramach sieci prywatnej pomiędzy stronami za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów.
Wdrożenie – świadczenia Wykonawcy mające na celu wykonanie Systemu.
Wsparcie – gwarantowana przez Wykonawcę i udzielana Zamawiającemu pomoc w eksploatacji (w tym prawo korzystania przez każdego z pracowników Zamawiającego z zdalnej pomocy helpdesk/telefon), prawo do otrzymywania Aktualizacji oraz usuwanie ewentualnych usterek Systemu na warunkach określonych w rozdziale pt. „Ogólne warunki gwarancji", wsparcie merytoryczne opisane w rozdziale "Audyt postępowania z dokumentacją, szkolenie z przepisów prawa, konsultacje merytoryczne".
Wzór dokumentu elektronicznego – Wzór pisma w formie Dokumentu Elektronicznego w rozumieniu Art.19 b) ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r., poz. 346 tj..) oraz §18 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 roku w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz. U. z 2019r., poz. 700).
XML – Format XML jest to obecnie powszechnie uznany standard publiczny, umożliwiający wymianę danych między różnymi systemami.
KSeF - Krajowy System e-Faktur.
PEF - Platforma Elektronicznego Fakturowania.
SZBI – Teleinformatyczny System Zarządzania Bezpieczeństwem Informacji modułu Kontroli Zarządczej w ramach posiadanego systemy elektroniczne zarządzanie dokumentacją.
KZ - modułu Kontroli Zarządczej w ramach posiadanego systemu elektroniczne zarządzanie dokumentacją.

PODSTAWY PRAWNE

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
2. Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 z późn. zm.).
3. Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011 nr 159, poz. 948 z późn. zm.).
4. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r., poz. 2509).
5. Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (tj.. Dz. U 2024 poz. 307)
6. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj.. Dz. U. z 2017 r., poz. 2247 z późn. zm.)
7. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji

elektronicznej (Dz. U. 2021 poz. 1797 z późn. zm.) (tj.. Dz. U. 2024 poz. 422)

8. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tj.. Dz. U. z 2020 r. poz. 344 z późn. zm.)
9. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (tj.. Dz. U. 2023 r. poz. 285 z późn. zm.).
10. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. 2006 r. Nr 206 poz. 1517 z późn. zm.).
11. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (tj.. Dz.U. 2024 poz. 422)
12. Ustawa z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (tj.. Dz. U. 2020 poz. 164).
13. Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. 2011 nr 14 poz. 67 oraz Dz. U. 2011 nr 27 poz. 140).
14. Ustawa z dnia 14 czerwca Kodeks Postępowania Administracyjnego (tj.. Dz.U. 2024 poz. 572)
15. Ustawa z dnia 29 sierpnia 1997 r. ordynacja (tj.. Dz.U. 2023 poz. 2383 z późn. zm.)
16. Ustawa z dnia 30 października 2002 r. o podatku leśnym (tj.. Dz. U. z 2019 poz. 888)
17. Ustawa z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (tj.. Dz. U. z 2023 poz. 70)
18. Ustawa z dnia 15 listopada 1984 . o podatku rolnym (tj.. Dz. U. z 2020 poz. 333 z późn. zm.)
19. Ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (tj.. Dz.U. 2024 poz. 399)
20. Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (tj.. Dz.U. 2024 poz. 609)
21. Ustawa z 27 kwietnia 2001 r. Prawo ochrony środowiska ((tj.. Dz.U. 2024 poz. 54).
22. Ustawa z 27 marca 2003 r. o planowaniu i zagospodarowaniu (tj.. Dz.U. 2023 poz. 977 z późn. zm.).
23. Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (tj.. Dz.U. 2023 poz. 1094 z późn. zm.).
24. Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i wolontariacie (tj.. Dz.U. 2023 poz. 571).
25. Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług (tj.. Dz.U. 2024 poz. 361).
26. Rozporządzenie Ministra Finansów z dnia 18 czerwca 2019 r. w sprawie sposobu przesyłania informacji o nieruchomościach i obiektach budowlanych oraz deklaracji na podatek od nieruchomości za pomocą środków komunikacji elektronicznej (Dz.U. 2019 poz. 1185 z późn. zm.).
27. Rozporządzenie Ministra Finansów z dnia 30 maja 2019 r. w sprawie wzorów informacji o nieruchomościach i obiektach budowlanych oraz

deklaracji na podatek od nieruchomości (Dz.U. 2019 poz. 1104 z późn. zm.).
28. Rozporządzenie Ministra Finansów z dnia 6 czerwca 2019 r. w sprawie sposobu przesyłania informacji o gruntach oraz deklaracji na podatek rolny za pomocą środków komunikacji elektronicznej (Dz.U. 2019 poz. 1153 z późn. zm.).
29. Rozporządzenie Ministra Finansów z dnia 30 maja 2019 r. w sprawie wzorów informacji o gruntach i deklaracji na podatek rolny (Dz.U. 2019 poz. 1105 z późn. zm.).
30. Rozporządzenie Ministra Finansów z dnia 3 czerwca 2019 r. w sprawie wzorów informacji o lasach i deklaracji na podatek leśny (Dz.U. 2019 poz. 1126 z późn. zm.).
31. Rozporządzenie Ministra Finansów z dnia 6 czerwca 2019 r. w sprawie sposobu przesyłania informacji o lasach oraz deklaracji na podatek leśny za pomocą środków komunikacji elektronicznej (Dz.U. 2019 poz. 1154 z późn. zm.).
32. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (tj.. Dz.U. 2023 poz. 1440).
33. Ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (tj. Dz.U. z 2022 poz. 2240 z późn. zm.).
34. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (tj.. Dz.U. z 2022 r. poz. 902).
35. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz.U. 2007 nr 10 poz. 68).
36. Ustawa z dnia 24 września 2010 r. o ewidencji ludności (tj.. Dz.U. 2024 poz. 736).
37. Ustawa z dnia 5 stycznia 2011 r. – Kodeks wyborczy (tj.. Dz.U. 2023 poz. 2408).

INFORMACJE OGÓLNE

Przedmiotem zamówienia jest wdrożenie kompleksowego Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO/IEC 27001 lub równoważną poprzez rozbudowę, modernizację i aktualizację modułu Kontrola Zarządcza, który jest częścią posiadanego przez Zamawiającego systemu e-Kancelaria http://gsko.unislaw.pl/.

1. Cel Zamówienia:

Celem niniejszego zamówienia jest wdrożenie kompleksowego Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO/IEC 27001 lub równoważną. System ma zapewniać najwyższy poziom ochrony danych, minimalizować ryzyko oraz gwarantować zgodność z przepisami prawnymi dotyczącymi ochrony danych osobowych i bezpieczeństwa informacji. Wdrożenie Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji będzie rozbudową modułu Kontroli Zarządczej w ramach posiadanego przez Zamawiającego systemu e-Kancelaria http://gsko.unislaw.pl/.

2. Zakres Przedmiotu Zamówienia:

2.1 Analiza Stanu Obecnego:

System powinien umożliwiać przeprowadzenie szczegółowej analizy aktualnego stanu bezpieczeństwa informacji w organizacji, obejmującej ocenę ryzyk, audyt bezpieczeństwa oraz identyfikację luk i słabych punktów.

2.2 Projektowanie SZBI:

System powinien umożliwiać opracowanie i przedstawienie projektu SZBI, w tym polityk, procedur oraz planów awaryjnych zgodnie z normą ISO/IEC 27001 lub równoważną. Moduł powinien wspierać definiowanie celów, strategii i wytycznych dotyczących bezpieczeństwa informacji.

2.3 Wdrożenie SZBI:

System powinien umożliwiać implementację zaprojektowanego systemu, obejmującą instalację niezbędnych narzędzi informatycznych, szkolenie personelu oraz uruchomienie procedur zarządzania bezpieczeństwem informacji. System powinien wspierać konfigurację i dostosowanie narzędzi do specyficznych potrzeb organizacji.

2.4 Monitorowanie i Audyt:

System powinien umożliwiać ustanowienie mechanizmów monitorowania zgodności systemu z przyjętymi politykami oraz przeprowadzanie regularnych audytów wewnętrznych i zewnętrznych. System powinien wspierać powiadomienia o niezgodnościach i generowanie raportów z audytów.

2.5 Ciągłe Doskonalenie:

System powinien umożliwiać zapewnienie mechanizmów ciągłego doskonalenia systemu, w tym analiza incydentów, regularne aktualizacje procedur oraz prowadzenie szkoleń doskonalących dla pracowników. System powinien wspierać raportowanie o postępach i wprowadzanych zmianach.

3. Wymagania Organizacyjne:

3.1 Polityki Bezpieczeństwa:

System powinien umożliwiać opracowanie i wdrożenie kompleksowych polityk bezpieczeństwa informacji, w tym polityki ochrony danych osobowych, polityki klasyfikacji informacji oraz polityki zarządzania ryzykiem. System powinien wspierać cykliczną rewizję i aktualizację polityk.

4. Szkolenia i Świadomość:

4.1 System powinien umożliwiać przeprowadzenie szkoleń dla pracowników na wszystkich poziomach organizacji w zakresie bezpieczeństwa informacji oraz podnoszenie świadomości zagrożeń związanych z cyberbezpieczeństwem. System powinien wspierać zarządzanie harmonogramem szkoleń i śledzenie ich realizacji.

4.2 Zarządzanie Incydentami:

System powinien umożliwiać opracowanie procedur zarządzania incydentami bezpieczeństwa, w tym procedur reakcji na incydenty, analizę przyczyn źródłowych oraz planów naprawczych. System powinien wspierać rejestrację i śledzenie incydentów oraz generowanie raportów z podjętych działań.

4.3 Zgodność z Przepisami:

System powinien umożliwiać zapewnienie zgodności z obowiązującymi przepisami prawnymi i regulacjami dotyczącymi ochrony danych osobowych oraz bezpieczeństwa informacji, w tym RODO oraz ustawą o ochronie danych osobowych. System powinien wspierać automatyczne aktualizacje zgodnie ze zmianami prawnymi.

5. Wymagania Dotyczące Dokumentacji:

5.1 Dokumentacja Polityk i Procedur:

System powinien umożliwiać opracowanie i dostarczenie dokumentacji polityk, procedur oraz instrukcji operacyjnych związanych z zarządzaniem bezpieczeństwem informacji. System powinien wspierać zarządzanie wersjami dokumentów.

5.2 Raporty z Audytów:

System powinien umożliwiać przedstawianie regularnych raportów z przeprowadzonych audytów bezpieczeństwa oraz ocen zgodności systemu z normą ISO/IEC 27001 lub równoważną. System powinien wspierać generowanie i archiwizację raportów.

Realizacja powyższych wytycznych powinna odbywać się poprzez następujące moduły: MODUŁ ZARZĄDZANIA RYZYKIEM

1. Moduł zarządzania ryzykiem pomaga kontrolować cały proces związany z zarządzaniem ryzykiem, już od chwili identyfikacji ryzyka poprzez jego obsługę w rejestrze, aż do momentu wygenerowania mapy ryzyka.
2. Moduł zarządzania ryzykiem w szczególności obejmuje:
   - Definiowanie rejestru ryzyk przez jednostkę;
   - Modyfikowanie rejestru ryzyk poprzez dopisywanie nowych pozycji ukrywanie widoczności nieaktualnych;
   - Możliwość zgłaszania ryzyka przez każdego pracownika;
   - Możliwość dodawania zgłoszonego ryzyka do rejestru;
3. Dzięki wykorzystaniu modułu zarządzania ryzykiem jednostka będzie mogła:
   - Zarządzać ryzykiem w sposób systemowy i tym samym realizować ustawowy obowiązek;
   - Przekazać kierownictwu jednostki rzetelną informację o ryzyku i na jej podstawie sformułować wstępne decyzje o charakterze zarządczym;
   - Wygenerować mapę ryzyka, która jest graficzną prezentacją ryzyka w momencie pierwotnym i po zastosowaniu mechanizmów redukujących ryzyko;

Moduł zarządzania ryzykiem umożliwia sprawozdawczość dającą pełną kontrolę nad ryzykiem mogącym wystąpić w jednostce.

MODUŁ LIST PYTAŃ KONTROLNYCH

1. System umożliwia prowadzenie bieżącego testu zgodności z przepisami prawa i innymi regulacjami.
2. Użytkownik ma możliwość tworzenia własnych list pytań kontrolnych lub skorzystania z gotowych list przygotowanych przez ekspertów z danej dziedziny (tj. zamówień publicznych, cyberbezpieczeństwa, norm ISO), w tym także przy użyciu wagowania istotności odpowiedzi.
3. Listy pytań kontrolnych są powiązane z jednostką redakcyjną podstawy prawnej lub orzeczenia, do której odwołują się poszczególne pytania w listach.
4. Listy pytań kontrolnych mogą być na bieżąco aktualizowane przez producenta - dopasowywane do zmieniających się przepisów; użytkownicy otrzymują informacje w systemie o zaktualizowanej liście pytań.
5. System w przejrzysty sposób prezentuje wyniki z wykonanych badań zgodności, wyszczególniając wszystkie zidentyfikowane niezgodności.

MODUŁ ZADAŃ

1. Proces przeprowadzania badania zgodności w szczególności obejmuje:

- Możliwość zdalnego wydawania przez wskazane w organizacji osoby poleceń wykonania analizy,
  badania, raportu, sprawozdania;
- Możliwość kierowania dowolnych zadań do pracowników na każdym poziomie organizacji, w tym zadań cyklicznych;
- Możliwość kierowania zadań w formie checklist do pracowników na każdym poziomie odpowiedzialności, aby określić stopień zgodności w wykonywanych zadaniach;
- możliwość dołączania do zadań delegowanych plików z wewnętrznymi procedurami placówki;
- Możliwość automatycznego powiadamiania określonych w poleceniu użytkowników o konieczności przygotowania sprawozdania, wypełnienia listy kontrolnej, nowych wiadomościach i ogłoszeniach;
- Możliwość generowania sprawozdań z wykonywanych zadań, w których parametrem będzie poziom zgodności z konkretną regulacją;

2. Dzięki zastosowanym mechanizmom zadaniowania i listom pytań kontrolnych Jednostka będzie mogła:

- Sprawdzić zgodność działania jednostki/komórki organizacyjnej z obowiązującym prawem lub regulacjami określonymi w części prezentującej zawartość kontentu merytorycznego;
- Weryfikować pojawiające się niezgodności w procesach i stopień zgodności w wykonywanych
  zadaniach;
- Reagować na ryzyko niezgodności poprzez delegowanie pracownikom, za pomocą systemu, konkretnych zadań redukujących niezgodność i śledzących skuteczność i czas ich wykonania;
- Na bieżąco monitorować działania pracowników w zakresie zadań przydzielonych w systemie;

3. W ramach modułu zadań system umożliwia raportowanie z realizowanych zadań i projektów we wszystkich obszarach i obowiązkach, wynikających z funkcjonowania jednostki samorządu terytorialnego. System prezentuje dwa rodzaje raportów - raporty statystyczne i przeglądowe. Moduł
   Raporty pozwala na:

- Ustalenie, co zostało wykonane w systemie np. w ramach danego zadania;
- Monitorowanie co i w jakich zakresach, zostało wykonane, jak duże są ewentualne zaległości oraz którzy pracownicy wykazują się największą aktywnością;
- Możliwość automatycznego tworzenie raportów w czasie rzeczywistym.

MODUŁ ANKIET

Modułem wspierającym bieżące utrzymywanie zgodności jest moduł ankiet, który umożliwia:

- Tworzenie ankiet zawierających pytania jednokrotnego, wielokrotnego wyboru, z listy rozwijanej oraz
  pytania otwarte;
- Po utworzeniu ankiety wysłanie informacji o dostępności ankiety w systemie poprzez wewnętrzny komunikator;

- Wykorzystanie kreatora ankiet i analizatora ankiet ułatwiającego przygotowanie narzędzi do analizy i oceny;
  Korzystanie z kalendarza pozwalającego na bezkolizyjne ustalenie terminów wykonania określonych działań;
- Włączenie opcji anonimowej ankiety podczas jej opracowania, co powinno być sygnalizowane w systemie przy jej wypełnianiu;
- Określanie terminu dostępności ankiety i jej automatyczne zamykanie po wygaśnięciu terminu wypełnienia;
- Dostęp do archiwum ankiet, raportów, sprawozdań;
- Segregowanie ankiet, sprawozdań, raportów według dowolnych kategorii;
- Włączanie filtrów podczas opracowania statystyk ankiet, np. poszczególnych pytań z wybranej
  ankiety.

MODUŁ ZARZĄDZANIA NIEZGODNOŚCIAMI (ZDARZENIAMI ORGANIZACYJNYMI)

1. Moduł zarządzania zdarzeniami organizacyjnymi umożliwia zgłaszanie zdarzeń organizacyjnych (administracyjnych, bhp, IT itp.) przez każdego pracownika placówki, ich rejestrowanie oraz monitorowanie.
2. Moduł zarządzania zdarzeniami w szczególności obejmuje:
   - Definiowanie indywidualnych słowników zdarzeń i incydentów;
   - Przypisywanie właścicieli kategorii i podkategorii zdarzeń i incydentów
   - Możliwość zgłaszania zdarzeń przez użytkowników zalogowanych oraz anonimowo;
   - Możliwość dodawania zgłoszonego naruszenia do rejestru;
   - Komentowanie zdarzeń w rejestrze;
   - Wysłania zadania z poziomu zgłoszonego naruszenia przez właściciela danej kategorii zgłoszenia;
   - Śledzenia historii zmian zdarzeń organizacyjnych oraz dokonanych w ramach zgłoszeń działań, zgłoszonych i w rejestrze;
3. Wykorzystanie modułu zarządzania zdarzeniami będzie wsparciem dla kierownictwa w zakresie:
   - Uzyskiwania rzetelnej informacji o obszarach zgłaszanych naruszeń i zdarzeń organizacyjnych;
   - Generowania raportów, analiz i statystyk oraz formułowania na ich podstawie decyzji o charakterze
   - zarządczym;
   - Wsparcia funkcji osoby odpowiedzialnej za monitorowanie wszystkich zdarzeń organizacyjnych i ewentualnego określania ryzyk dla placówki.

MODUŁ KOMUNIKATÓW

1. System zawiera elektroniczną tablicę ogłoszeń - ogłoszenia są automatycznie dezaktualizowane (o dacie decyduje osoba o przyznanych odpowiednich uprawnieniach). Każdy użytkownik systemu jest informowany o nowych ogłoszeniach;
2. System umożliwia wysłanie wiadomości do konkretnego pracownika, grupy pracowników czy też zespołów zadaniowych z potwierdzeniem odbioru takiej wiadomości;

Wymagania niefunkcjonalne:

1. EZD musi posiadać architekturę trójwarstwową:
   1) warstwa prezentacji, obejmująca interfejsy użytkownika klienta WWW,

2) warstwa aplikacji, obejmującą serwer Systemu,
3) warstwa danych, zawierającą serwer bazy danych.

2. Interfejs użytkownika systemu musi być w całości polskojęzyczny. W języku polskim muszą być również wyświetlane wszystkie komunikaty przekazywane przez System, włącznie z komunikatami o błędach.
3. EZD musi informować użytkownika w momencie zaciągania plików, że plik przekroczył dopuszczalny rozmiar.
4. EZD musi przechowywać wszystkie dane w bazie danych zgodnej ze standardem SQL oraz zapewniającej transakcyjność operacji. Dopuszcza się przechowywanie poza bazą danych plików, w postaci repozytorium dyskowego – ich integralność z systemem musi być zapewniona przez metadane opisujące poszczególne pliki. Metadane muszą być przechowywane w bazie danych.
5. EZD musi działać w środowiskach systemowych bazujących na technologii Microsoft Windows oraz w środowiskach opartych na systemie Linux.
6. EZD musi umożliwiać dostęp do systemu przez użytkownika końcowego z poziomu przeglądarki internetowej, co najmniej Firefox, Google Chrome, MS Edge, Safari w najnowszych wersjach.
7. EZD musi cechować się interfejsem użytkownika opartym na nowoczesnych rozwiązaniach: wykorzystywać menu, listy, formularze, przyciski, referencje (linki), itp.
8. Wymaga się, aby interfejs użytkownika EZD stosował oznaczanie pól wymaganych na formularzu ekranowym w sposób wyróżniający te pola, a w przypadku ich błędnego wypełnienia jednoznacznie wskazywał na pola błędnie wypełnione oraz informował o przyczynie błędu.
9. EZD musi cechować duża elastyczność, rozumiana jako możliwość dostosowania systemu do zmieniających się wymagań funkcjonalnych wynikających ze zmieniającego się stanu prawnego i zmieniających się warunków praktycznych i przepisów prawnych.
10. EZD musi zabezpieczać dane przed przypadkowym nadpisaniem w przypadku równoczesnego korzystania z tych danych przez wielu użytkowników.
11. EZD musi posiadać widok indywidualny, prezentujący tylko te składniki systemu, do których uprawniony jest dany użytkownik.
12. System musi umożliwiać integrację z Active Directory w trybie SSO (Single Sign On). Logowanie do systemu odbywa się automatycznie za pomocą danych z konta AD. Użytkownik po zalogowaniu do AD nie musi logować się drugi raz do systemu EZD (Jednokrotne logowanie).
13. EZD musi zapewniać możliwość:
    1) narzucenia minimalnej długości hasła oraz obowiązku wykorzystania różnych rodzajów znaków w haśle (np. liter, cyfr i znaków specjalnych);
    2) ustalenia czasu obowiązywania hasła;
    3) automatycznego odrzucania prób ustalenia przez użytkownika trywialnego hasła (np. imienia lub nazwiska użytkownika).
14. EZD musi być wyposażony w filtry umożliwiające wyszukanie odpowiednich dokumentów (i innych obiektów) oraz interesantów według predefiniowanych atrybutów (kryteriów wyszukiwania).
15. System EZD musi pozwalać na odbieranie i wysyłanie dowolnych dokumentów z i do zewnętrznych systemów za pośrednictwem skrytki ePUAP.

16. Środowisko EZD powinno umożliwiać udostępnianie usług WebService.
17. EZD musi zapewniać możliwość integracji z systemem ePUAP, automatyczną rejestrację i wysyłanie dokumentów, weryfikację podpisów i paczek ePUAP oraz wizualizacji dokumentów pobranych z ePUAP oraz UPO, UPD i UPP.
18. EZD musi zapewnić podpisywanie pojedynczych i wielu pism i załączników podpisem elektronicznym kwalifikowanym z poziomu aplikacji, weryfikację podpisu.
19. EZD musi zapewniać możliwość podpisywania pism za pomocą Podpisu Zaufanego (PZ).
20. EZD musi zapewniać możliwość podpisywania pism i załączników za pomocą kwalifikowanej pieczęci elektronicznej.
21. EZD musi zapewniać współpracę z urządzeniami wspomagającymi rejestrację dokumentów, a w szczególności: skanerami; czytnikami kodów kreskowych; drukarkami etykiet adresowych i kodów kreskowych, tabletem do podpisu
22. EZD musi umożliwiać definiowanie uprawnień każdego ze stanowisk w zakresie: dostępu do odpowiednich modułów, w tym dokumentów i spraw oraz uprawnień do aktualizacji i przeglądania ich zawartości.
23. EZD musi umożliwiać wymuszanie zmiany hasła po upływie czasu, określonego przez Administratora.
24. EZD musi cechować się rozbudowanym modułem bezpieczeństwa zarządzającym dostępem użytkowników do funkcji systemu. Musi zapewnić dostęp do wybranych funkcji administracyjnych dla uprawnionych pracowników.
25. Panel administracyjny EZD musi umożliwiać uprawnionym Użytkownikom zdefiniowanie i prowadzenie rejestrów wszystkich typów dokumentów z zakresu działalności Zamawiającego zgodnie z wymaganiami prawnymi dotyczącymi tych dokumentów (np. ewidencja decyzji, zaświadczeń itd.).
26. EZD musi zapewnić: odwzorowanie struktury organizacyjnej urzędu (komórek, pracowników, stanowisk) z możliwością modyfikacji, przydzielanie zdefiniowanym grupom użytkowników uprawnień do wykonywania określonych funkcji.
27. Panel administracyjny EZD musi umożliwiać przeglądanie historii logowania użytkowników.
28. EZD musi umożliwiać zarządzanie słownikiem Jednolitego Rzeczowego Wykazu Akt i nadawanie uprawnień dla poszczególnych klas.
29. Panel administracyjny EZD musi umożliwiać zarządzanie kontami, w minimalnym zakresie:
    1) edycji uprawnień,
    2) musi umożliwiać zarządzanie i określanie przez Administratora wymaganej złożoności hasła,
    3) określanie co najmniej: maksymalnej i minimalnej długości hasła, czasu ważności hasła,
    4) ustawienia praw dostępu dla stanowiska.
30. EZD musi zapewniać funkcjonalność zarządzania dostępem do aplikacji:
    1) Administrator systemu musi mieć możliwość tworzenia, modyfikacji oraz dezaktywacji kont użytkowników,
    2) Administrator systemu, użytkownik może nadawać uprawnienia innym użytkownikom,
    3) Administrator systemu może przypisywać użytkowników do grup,
31. System musi pozwalać na wygenerowanie linka do zmiany hasła dla

użytkownika.

Wymagania funkcjonalne

1. System musi umożliwiać pracę w trzech trybach:
   1) w trybie wspierającym obieg dokumentów papierowych,
   2) w trybie EZD,
   3) w trybie mieszanym.
2. EZD musi obsługiwać rejestrację przesyłek przychodzących, w formie papierowej i elektronicznej (przekazywanych za pośrednictwem Elektronicznej Skrzynki Podawczej na ePUAP, portalu e-usług lub innych skrzynek podawczych oraz poczty elektronicznej).
3. System EZD musi być zintegrowany z usługą e-Doręczeń elektronicznych umożliwiając:
   1) odbieranie, jak i wysyłanie dokumentów poprzez e-Doręczenia elektroniczne,
   2) obsługę wszystkich formatów dokumentów wymagane przez platformę e-Doręczeń
   3) Śledzenie statusów doręczeń (np. dostarczone, odebrane, odrzucone) i informowanie użytkowników o zmianach statusów za pomocą powiadomień systemowych,
4. System EZD musi obsługiwać procesy wysyłania i odbierania dokumentów metodą hybrydową (PUH), które obejmują formę tradycyjną (papierową) a w szczególności:
   1) Umożliwiać automatyczne przekształcanie dokumentów elektronicznych do formatu umożliwiającego prawidłowe wysłanie dokumentu,
   2) umożliwiać śledzenie statusów doręczeń hybrydowych w sposób ciągły, z aktualizacją informacji o doręczeniach papierowych (np. potwierdzenia odbioru zwracane do systemu).
5. System EZD musi być zintegrowany z Platformą Elektronicznego Fakturowania (PEF) w celu odbierania, wysyłania i przetwarzania faktur elektronicznych oraz musi obsługiwać formaty dokumentów zgodne z europejskim standardem e-fakturowania.
6. System EZD musi być zintegrowany z Krajowym Systemem e-Faktur (KSeF) w celu wymiany faktur elektronicznych zgodnie z wymogami ustawowymi oraz wspierać procesy wysyłania, odbierania i archiwizacji e-faktur zgodnie z wymogami KSeF.
7. System EZD musi umożliwiać doręczenia korespondencji metodą gońcową wraz z wykorzystaniem do obsługi gońców aplikacji mobilnej a w szczególności:
   1) Umożliwiać tworzenie rejonów dostawczych i przypisywanie konkretnych gońców do obsługi poszczególnych rejonów,
   2) Pozwalać na przydzielanie zadań doręczeniowych do konkretnych gońców, z możliwością śledzenia realizacji tych zadań,
   3) Umożliwiać rejestrowanie potwierdzeń doręczeń za pomocą urządzeń mobilnych, w tym zbierania podpisów odbiorców na ekranach urządzeń mobilnych z funkcją zapisywania danych geolokalizacyjnych,
   4) Aplikacja mobilna musi umożliwiać gońcom zarządzanie zadaniami doręczeniowymi, rejestrowanie doręczeń oraz komunikację z centralnym systemem EZD,
   5) Umożliwiać gońcom synchronizację danych pomiędzy aplikacją mobilną a centralnym systemem EZD, w tym aktualizację statusów doręczeń i

raportowanie postępów realizacji zadań,

6) Umożliwiać generowanie raportów dotyczących działalności gońców, obejmujących m.in. liczbę doręczonych przesyłek oraz skuteczność doręczeń.

8. System EZD musi wspierać obsługę wysyłek z wykorzystaniem systemu E-nadawca Poczty Polskiej - wysyłka przesyłek krajowych i zagranicznych, obsługa EPO
9. Podczas procesu rejestracji przesyłek przychodzących w formie papierowej, EZD musi umożliwiać skanowanie z wykorzystaniem skanera zgodnego z TWAIN (z poziomu interfejsu aplikacji) poszczególnych dokumentów, wchodzących w skład przesyłki. Interfejs do skanowania musi posiadać co najmniej narzędzia do edycji obrazu ze skanera poprzez: obrót o dowolny kąt, zmianę kolejności stron, zapis do PNG i PDF, zmiany kontrastu.
10. Podczas rejestracji przesyłek przychodzących w formie papierowej , EZD musi umożliwiać skanowanie wsadowe.
11. System musi wspierać integrację z programami ABC Pro – Legislator oraz Anon
12. EZD musi umożliwiać odebranie poczty elektronicznej za pomocą wbudowanego klienta pocztowego IMAP oraz SMTP i umożliwić rejestrację w rejestrze przesyłek wpływających lub bezpośrednie dołączenie wiadomości z załącznikami do akt sprawy.
13. EZD musi umożliwiać opatrywanie przesyłek przychodzących metadanymi zgodnie z instrukcją kancelaryjną.
14. System musi umożliwiać generowanie potwierdzenia przyjęcia przesyłki wpływającej przez punkt kancelaryjny, opatrzonego kodem kreskowym odpowiadającym kodowi kreskowemu przesyłki. Potwierdzenie przyjęcia wygenerowane przez EZD musi umożliwiać zamieszczenie co najmniej daty wpływu, oznaczenia graficznego jednostki, nazwy jednostki.
15. EZD musi umożliwiać rejestrację zwrotów przesyłek oraz pocztowych potwierdzeń odbioru (zwrotek).
16. System EZD musi wspierać funkcjonalność składania podpisu elektronicznego na urządzeniach mobilnych, takich jak tablety, podczas odbioru dokumentów w urzędzie.
17. System EZD musi umożliwiać tworzenie tzw. kancelarii wydziałowych składających się z grup pracowników odpowiedzialnych za rejestrację dokumentów przychodzących w obrębie danego wydziału lub komórki organizacyjnej.
18. Administrator EZD musi mieć możliwość elastycznego definiowania struktur kancelarii wydziałowych, dostosowując je do specyficznych potrzeb urzędu i poszczególnych komórek organizacyjnych.
19. EZD musi umożliwiać zarządzanie zakresem zawartości słowników systemowych. Minimalna lista słowników to: JRWA, Gońcy, Rejony, Kody pocztowe, Rodzaje dokumentów, Sposoby dostarczania korespondencji, Sposoby wysyłania korespondencji, Statusy spraw, Sposoby płatności, rodzaje interesantów.
20. EZD musi umożliwiać użytkownikom dekretującym wskazanie jednej lub kilku komórek lub stanowisk merytorycznych odpowiedzialnych za prowadzenie i zakończenie sprawy. W przypadku wyboru kilku osób, możliwe jest wskazanie osoby odpowiedzialnej za ostateczne załatwienie sprawy.
21. EZD musi umożliwiać przekazywanie dokumentów na pojedyncze stanowiska i

na wiele stanowisk.

22. System musi pozwalać na wprowadzenie polecenia kierowanego do wszystkich adresatów dekretacji i indywidualnego polecenia dla każdego adresata.
23. EZD musi umożliwiać dekretacje dokumentu ze wskazaniem komórki wiodącej, współpracującej oraz do wiadomości.
24. EZD musi umożliwiać tworzenie kopii dokumentu na podstawie oryginału, kopii i do wiadomości.
25. Utworzona kopia powinna mieć właściwości maksymalnie takie jak dokument, w oparciu o który powstała (np. z dokumentu do wiadomości nie może powstać kopia).
26. System musi pilnować, by dokument w trakcie kolejnych dekretacji był zadekretowany maksymalnie z ustawieniem takimi, jak został zadekretowany krok wcześniej (np. w przypadku pierwszej dekretacji kopii dokumentu, kolejna dekretacja nie może się odbyć na oryginale na stanowisku, które otrzymało kopię).
27. EZD powinno pozwalać administratorom na zdefiniowanie domyślnej grupy osób, do których dekretowany będzie dokument.
28. EZD musi umożliwić odróżnienie oraz jednoznaczną identyfikację i odrębne przetwarzanie poszczególnych dokumentów, przechowywanych w postaci odwzorowań cyfrowych wchodzących w skład przesyłki, przy zachowaniu ich powiązania z przesyłką.
29. EZD musi umożliwić dodawanie przez użytkownika informacji opisujących poszczególne dokumenty, przesyłki lub sprawy w postaci notatek, zgodnie z instrukcją kancelaryjną.
30. EZD musi umożliwiać dwustronną komunikację z systemem ePUAP (odbieranie – wysyłanie dokumentów).
31. EZD musi automatyczne przypisywać UPP i UPD do wysłanych dokumentów przez ESP.
32. EZD musi posiadać wbudowany edytor tworzenia szablonów dokumentów służący do tworzenia
    dokumentów wewnątrz systemu, bez konieczności używania zewnętrznych aplikacji.
33. EZD musi obsługiwać szablony dokumentów co najmniej w zakresie:
    1) możliwości zdefiniowania szablonu dokumentu oraz przypisania do niego uprawnień dla stanowisk lub komórek organizacyjnych,
    2) możliwość tworzenia szablonów w zależności od typu dokumentu: korespondencja wychodząca, dokument wpływający, dokument wewnętrzny,
    3) prowadzenia repozytorium szablonów, które umożliwia zarządzanie szablonami,
    4) możliwości wstawiania znaczników do szablonu. Minimalny zakres znaczników:
        a) dane nadawcy,
        b) dane adresata (min. imię, nazwisko, adres, nazwa instytucji),
        c) kod kreskowy,
        d) pełne dane pracownika prowadzącego sprawę,
        e) znak pisma/sprawy,
        f) adresaci pisma,

g) data pisma,
h) lista stron sprawy,
i) elementy pozwalające na sterowanie zawartością dokumentu np. znacznik nowej strony,

5) możliwości wykorzystania zdefiniowanego szablonu przy tworzeniu pism wychodzących z autouzupełnianiem zawartości w/w znaczników,
6) możliwości generowania korespondencji seryjnej.

34. Każdy dokument opiera się o indywidualny szablon dokumentu, który jest definiowany w systemie.
35. Każdy szablon może posiadać dowolną liczbę kontrolek.
36. W przypadku rejestracji dokumentu XML (zgodnego z CRD) system musi automatycznie kopiować dane z poszczególnych węzłów dokumentu XML do odpowiednich kontrolek.
37. System musi umożliwić eksport dokumentu systemowego do następujących formatów: XML (zgodnego z CRD), PDF, DOCX, ODT.
38. EZD musi umożliwiać integrację z pakietem MS Office, OpenOffice i LibreOffice co najmniej w zakresie możliwości edycji dokumentów wychodzących (pisma, arkusze) dołączanych przez użytkowników do spraw bezpośrednio w pakiecie MS Office, OpenOffice i LibreOffice, EZD musi umożliwiać import tekstu przygotowanego w zewnętrznym procesorze tekstu.
39. EZD musi umożliwić generowanie i drukowanie nalepek z kodami kreskowymi na dokumenty papierowe oraz nośniki i odnajdywanie na podstawie zeskanowanej nalepki odwzorowania cyfrowego bądź metryki danego dokumentu.
40. EZD musi umożliwiać generowanie kopert/naklejek dla korespondencji wychodzącej wraz z kodem kreskowym zawierającym unikatowy identyfikator wysyłki.
41. System musi pozwalać na łączenie wielu przesyłek wychodzących w jedną kopertę, w przypadku, gdy użytkownik stwierdzi, iż dotyczą one tego samego adresata.
42. EZD musi być zintegrowane z programem obsługującym pocztę tradycyjną w zakresie automatycznego przesyłania listy przesyłek oraz odbioru z tejże aplikacji, informacji o numerze nadanym przesyłce, doręczeniu, ZPO lub zwrocie przesyłki. System musi umożliwiać wydruk książki nadawczej oraz dziennika korespondencji.
43. System musi umożliwiać tworzenie własnych cenników przesyłek uwzględniających formę wysyłki, wagę i gabaryt.
44. EZD musi prezentować informacje na temat statusu przeczytania zadekretowanego/przekazanego dokumentu i na tej podstawie umożliwiać cofnięcie wykonanej czynności.
45. EZD musi umożliwić rejestrację historii pisma (czynność wykonana, data i czas, użytkownik) dokumentów papierowych (dla których istnieje odwzorowanie cyfrowe oraz dla których nie zostało ono wykonane) oraz nośników.
46. EZD musi umożliwić wszczynanie, prowadzenie i załatwianie spraw, przechowywanie akt sprawy i prowadzenie spisów spraw zgodnie z obowiązującymi przepisami. System automatycznie musi nadawać znak sprawy i zapewnia jego zgodność z wymogami instrukcji kancelaryjnej.
47. EZD musi umożliwić prowadzenie rejestrów kancelaryjnych, w tym rejestru

przesyłek wpływających, wychodzących oraz pism wewnętrznych.

48. EZD musi umożliwić numerację i klasyfikację spraw w oparciu o JRWA zgodnie z instrukcją kancelaryjną.
49. EZD musi umożliwiać określenie terminu realizacji spraw w oparciu o dane JRWA.
50. EZD musi umożliwiać oddzielną rejestrację dokumentów nietworzących akt sprawy, w szczególności:
    1) rejestru faktur – wyposażonego w opcję wieloetapowego zatwierdzania faktury i potwierdzania płatności faktury przez uprawnionych użytkowników wraz z mechanizmem wizualnego oznaczania faktur przeterminowanych,
    2) definiowania z poziomu administratora systemu dowolnego rejestru poprzez:
    3) definicję pól i typów pól dokumentów wchodzących w skład rejestru,
    4) możliwość definiowania masek w polach rejestru,
    5) definiowanie uprawnień (podglądu, edycji),
    6) możliwość udostępnienia zawartości rejestru na BIP.
51. EZD musi umożliwiać wielostopniowy proces akceptacji dokumentów (zgodnie z instrukcją kancelaryjną podmiotu), z możliwością parametryzacji wymagalności akceptacji dla dokumentu przed jego wysłaniem do interesanta. System musi mieć możliwość wymuszenia przez użytkownika dokonania akceptacji dokumentu z podpisem (podpisem zaufanym, podpisem kwalifikowanym, pieczęcią elektroniczną).
52. EZD musi zapewniać możliwość podpisywania pism i załączników za pomocą kwalifikowanej pieczęci elektronicznej w postaci dostępu zdalnego (chmurowego). Pieczęć jest przetrzymywana na przeznaczonym do tego celu bezpiecznym urządzeniu HSM znajdującym się w infrastrukturze Kwalifikowanego Dostawcy Usług Zaufania. Dostęp do pieczęci musi być odpowiednio szyfrowany i wymagać odpowiedniej autoryzacji przed rozpoczęciem . Za pomocą usługi dostarczonej w takim modelu jest możliwość automatyzacji procesu sygnowania dokumentów. W ramach tej usługi wykonawca dostarczy niezbędne oprogramowanie do podpisywania pieczęcią kwalifikowaną oraz zapewni minimum 5 000 użyć pieczęci przez okres 1 roku
53. Użytkownik powinien mieć możliwość swobodnego definiowania ścieżek akceptacji (wskazania konkretnych osób oraz liczby pozytywnych zatwierdzeń dla każdego etapu akceptacji).
54. EZD musi umożliwić zapis projektów pism przekazywanych pomiędzy użytkownikami lub komórkami w trakcie załatwiania sprawy, a także zamieszczanie komentarzy odnoszących się do projektów pism.
55. EZD musi zapewnić prowadzenie, podgląd oraz wydruk metryki sprawy zgodnie z obowiązującymi
    przepisami.
56. EZD musi umożliwić opisywanie spraw i akt sprawy metadanymi zgodnie z obowiązującymi przepisami.
57. EZD musi umożliwić odnotowanie wysyłki przesyłek wychodzących w rejestrze i opatrzenie ich metadanymi
    zgodnie z przepisami.
58. EZD musi zapewnić przydzielanie spraw i korespondencji, przekazanych na dane stanowisko, konkretnym
    użytkownikom pracującym na tym stanowisku.
59. EZD musi umożliwić podgląd historii sprawy, ścieżki obiegu sprawy w taki

sposób by możliwe było odwzorowanie pełnego przebiegu sprawy.

60. EZD musi umożliwiać grupowanie dynamiczne spraw w projekty, określenie członków grupy projektowej oraz praw dostępu do projektu.
61. EZD musi posiadać funkcjonalność obsługi kalendarzy. Każdy z użytkowników powinien posiadać dostęp do własnego kalendarza z możliwością dodawania do niego dowolnych zdarzeń. Użytkownik powinien mieć możliwość określenia typu zdarzenia oraz jego opisu. Użytkownik powinien mieć również możliwość definiowania zdarzeń całodniowych i dłuższych oraz cyklicznych. System ma umożliwiać przeglądanie kalendarzy podwładnych. Kalendarz musi umożliwiać dodawanie i edycję wpisów za pomocą mechanizmu „przeciągnij i upuść".
62. EZD musi posiadać funkcjonalność planowania i raportowania spotkań, co najmniej w zakresie:
    1) opracowywanie agendy spotkania,
    2) zapraszanie uczestników,
    3) wyszukiwanie spotkań,
    4) pisanie raportów ze spotkań na podstawie agendy (również przy jej braku),
    5) zakładanie kolejnych spraw na podstawie protokołu za spotkania.
63. EZD musi umożliwiać zarządzanie zasobami poprzez ustalanie rezerwacji zasobów. System musi umożliwić definiowanie dowolnych zasobów. Każdy zasób musi być powiązany ze „swoim" terminarzem, do którego uprawnieni użytkownicy mają wgląd. Ponadto tylko uprawnieni użytkownicy mogą rezerwować zasoby, a fakt rezerwacji jest odnotowywany w terminarzu zasobu. Musi również istnieć możliwość grupowania zasobów (np. grupa „pojazdy" zawierająca pojazdy, którymi dysponuje Urząd).
64. EZD musi posiadać funkcjonalność pozwalającą na zbiorcze podejrzenie dostępności rezerwowanych zasobów i innych użytkowników. Każdy terminarz musi być możliwy do przeglądania w trybie dziennym, tygodniowym, miesięcznym.
65. EZD musi być wyposażony w funkcjonalność komunikatora tekstowego. Komunikator musi być integralnym elementem EZD. Komunikator musi umożliwić prowadzenie rozmów pomiędzy dwoma użytkownikami lub prowadzenie rozmów grupowych.
66. EZD musi umożliwić użytkownikowi podgląd przypisanych do niego spraw i korespondencji, z możliwością sortowania, filtrowania i przeszukiwania.
67. EZD musi mieć umożliwić wprowadzanie zmian kadrowych, urlopów i zastępstw. Umożliwia przekazanie osobie zastępującej części lub całości uprawnień osoby zastępowanej. Uprawnienia muszą być przekazane na określony czas dat lub bezterminowo.
68. EZD musi posiadać moduł urlopów umożliwiający co najmniej:
    1) obsługę wniosków urlopowych umożliwiającą złożenie wniosku przez pracownika oraz późniejszą akceptację przez kierownika oraz ostateczne zatwierdzenie przez kadrową,
    2) wyznaczanie zastępstw na podstawie udzielonych urlopów,
    3) integracje funkcjonalności urlopów z kalendarzem systemowym co najmniej w zakresie widoku planowanych urlopów, uzależnionego od posiadanych uprawnień tj., pracownik widzi swoje urlopy, kierownik widzi urlopy swoje jak i pracowników podległych, kadrowa widzi urlopy wszystkich

pracowników,
4) informowanie w momencie dekretacji o nieobecności pracownika, na którego dekretowany jest dokument.

69. EZD musi umożliwiać definiowanie zastępstw na czas nieobecności, polegających na udzieleniu pełnomocnictwa innemu użytkownikowi do wykonywania czynności w imieniu użytkownika nieobecnego. Pełnomocnictwo powinno być definiowane w określonym przedziale czasu. Dostęp do danych nieobecnego użytkownika powinien być kontrolowany przez System i odbierany wraz z upłynięciem daty końcowej. W trakcie trwania zastępstwa w systemie jest prezentowana informacja o zastępowaniu jednej osoby przez drugą. Wszystkie operacje wykonywane w zastępstwie powinny być zapisane w sposób umożliwiający jednoznaczne określenie, kto wykonał daną operację.
70. EZD musi posiadać moduł obsługi delegacji umożliwiający obsługę wniosków o delegację krajową i zagraniczną oraz późniejszą akceptację przez kierownika.
71. EZD musi umożliwiać przekazywanie spraw na inne stanowisko lub do innej komórki organizacyjnej.
72. EZD musi umożliwić prowadzenie książki teleadresowej interesantów.
73. EZD musi posiadać wewnętrzny edytor, służący do sporządzania komentarzy załączanych do akt sprawy.
74. System musi udostępniać zestaw raportów niezbędnych do pracy urzędu. Użytkownik musi mieć możliwość określenia podstawowych parametrów raportów (okres za jaki raport będzie generowany, sposób sortowania). System musi umożliwiać wygenerowanie co najmniej następujących raportów:
    1) Statystyki dla spraw;
    2) Statystyki dla pism:
    3) Raport pism przychodzących;
    4) Raport pism przekazanych na stanowisko;
    5) Raport pism wychodzących;
    6) Raport z książki doręczeń;
    7) Raport dekretacji;
    8) Raport zwrotów;
    9) Raport dokumentów interesanta;
    10) Raport udostępnień danych osobowych;
    11) Koszty wysyłek dokumentu;
    12) Raport terminowości pracowników.
75. Raporty muszą być zwizualizowane w postaci tabeli oraz wykresu.
76. Raporty można wygenerować dla całego urzędu, referatu, biura lub konkretnego pracownika.
77. EZD musi posiadać interfejsy komunikacyjne z Platformą usług informatycznych ePUAP – w zakresie dwukierunkowej integracji z usługą Elektronicznej Skrzynki Podawczej dostępną na ePUAP.
78. EZD ma mieć możliwość importu skrytek podawczych podmiotów z platformy ePUAP.
79. EZD musi posiadać moduł (funkcjonalność) zapewniający obsługę składów chronologicznych dla dokumentów papierowych, -archiwum zakładowe umożliwiające: przekazywania dokumentacji przez komórki organizacyjne do archiwum zakładowego, wypożyczania dokumentów, brakowania, wycofywania dokumentacji itd.
80. EZD musi umożliwić dokumentowanie wyjęcia dokumentacji ze składu

chronologicznego lub ze składu informatycznych nośników danych oraz wydrukowanie karty zastępczej dla wypożyczanego nośnika. Procedura obsługi składów powinna być realizowana w następujący sposób: pracownik sprawdza dostępność nośnika, a następnie składa wniosek o wypożyczenie, osoba obsługująca skład akceptuje wniosek i wypożycza nośnik, zwrot nośnika również jest potwierdzany przez osobę obsługującą skład.

81. EZD musi zapewnić przejmowanie dokumentacji przez archiwum zakładowe po upływie okresu przewidzianego w instrukcji kancelaryjnej lub ustalonego w podmiocie. Przejęcie dokumentacji musi polegać na przekazaniu archiwiście uprawnień do tej dokumentacji w systemie EZD oraz ograniczeniu uprawień komórki merytorycznej, zgodnie z instrukcją kancelaryjną.
82. EZD musi posiadać dedykowane funkcje do udostępniania i wycofywania dokumentacji elektronicznej z archiwum zakładowego.
83. EZD musi umożliwiać wypożyczanie spraw z archiwum, podgląd informacji o sprawie oraz zmianę kategorii archiwalnej sprawy przechowywanej w archiwum.
84. EZD musi posiadać funkcje wspierające proces porządkowania dokumentacji w archiwum zakładowym (wskazanie dokumentacji wymagającej uzupełnienia).
85. EZD musi realizować brakowanie akt elektronicznych oraz przekazanie akt do Archiwum Państwowego oraz sporządzenie i przechowywanie odpowiedniej dokumentacji.
86. EZD musi wspierać pracę archiwisty poprzez automatyczne typowanie dokumentacji do brakowania lub przekazania do archiwum państwowego (po upływie terminów związanych z danymi kategoriami archiwalnymi).
87. EZD musi wspomagać użytkownika w przygotowywaniu paczki archiwalnej dla Archiwum Państwowego poprzez przygotowywanie automatycznych spisów zdawczo-odbiorczych, wykazu akt, oraz zapisanie spraw w strukturze wymaganej przez Archiwum Państwowe.
88. EZD musi wspomagać użytkownika w przygotowywaniu paczki administracyjnej do przekazania między instytucjami administracji publicznej lub wewnątrz jednostki administracyjnej w formie elektronicznej, zawierającej wszystkie niezbędne dokumenty i metadane wymagane do kompletnej i zgodnej z przepisami wymiany informacji.
89. EZD musi wspomagać użytkownika w przygotowywaniu paczki sądowej do przekazania do sądu w formie elektronicznej, zgodnie z wymogami postępowania sądowego zawierającej wszystkie niezbędne dokumenty, załączniki oraz metadane wymagane przez sąd.
90. EZD musi umożliwiać sporządzenie pocztowej książki nadawczej dostosowanej do zróżnicowanych wymagań występujących w różnych urzędach pocztowych.
91. EZD musi posiadać wbudowany mechanizm powiadomień, informujący o istotnych zdarzeniach związanych z jego aktywnością w systemie. Minimalny zbiór powiadomień powinien obejmować informowanie o: zadekretowaniu dokumentu na pracownika, przekazaniu dokumentu do akceptacji, akceptacji dokumentu, udostępnieniu dokumentu pracownikowi.
92. EZD musi posiadać mechanizm parafowania dokumentów oraz podpisywania ich kwalifikowanym podpisem elektronicznym. W przypadku dokumentów podpisanych – istnieje możliwość weryfikacji złożonego podpisu oraz wydrukowania raportu z podpisu.
93. Klient ESP musi mieć możliwość obsługi wielu skrytek jednocześnie.

94. Klient ESP musi mieć możliwość wyświetlania dowolnego dokumentu XML. Jeśli dokument XML nie posiada wskazania na XSL lub wskazane XSL nie jest dostępne, klient ESP musi rozpoznać taką sytuację i wyświetlić wszystkie węzły tego dokumentu XML.
95. Klient ESP musi prawidłowo wyświetlać każdy dokument zgodny z CRD.
96. Klient ESP musi automatycznie wyłuskiwać następujące dane z dokumentu XML (zgodnego z CRD): załączniki, dane nadawcy i odbiorcy z węzła Dane Dokumentu oraz informacje o osobie, która podpisała dokument podpisem kwalifikowanym lub Profilem Zaufanym.
97. Klient ESP musi umożliwić automatyczne weryfikowanie podpisu złożonego za pomocą Podpisu Zaufanego.

Administracja systemem i warunki techniczne

1. EZD musi umożliwić modelowanie wielopoziomowej struktury organizacyjnej instytucji, która umożliwi przypisanie pracowników do odpowiednich stanowisk, a także wprowadzanie modyfikacji w strukturze w ramach zmian organizacyjnych za pomocą dezaktywacji i aktywacji stanowisk i komórek organizacyjnych.
2. EZD musi umożliwić definiowanie uprawnień do poszczególnych funkcji systemu oraz grupowanie uprawnień w role w celu ułatwienia administracji systemem.
3. Uprawnienia i role przypisywane są do stanowiska, a nie do użytkownika systemowego.
4. Użytkownik logując się do systemu, ma dostęp do określonych obszarów systemu na podstawie uprawnień, które posiada stanowisko, do którego jest przypisany użytkownik.
5. EZD musi umożliwiać delegowanie części lub całości posiadanych uprawnień.
6. System musi posiadać wyodrębniony moduł administracyjny. Dostęp do tego modułu mogą uzyskać jedynie użytkownicy z odpowiednimi uprawnieniami.
7. EZD musi posiadać rozbudowany rejestr zdarzeń rejestrujący akcje użytkowników na obiektach systemowych, udane i nieudane próby logowania oraz typowe błędy aplikacji.
8. EZD umożliwi zarządzanie uprawnieniami w oparciu o grupy uprawnień i grupy zasobów, jakich dotyczą. System uprawnień musi być zdolny do odzwierciedlenia uprawnień i odpowiedzialności poszczególnych pracowników wynikający z instrukcji kancelaryjnych oraz struktury stanowisk.
9. Hasła w EZD muszą być przechowywane w systemie w formie zaszyfrowanej - nie może być możliwości ich odtworzenia, lecz jedynie zresetowania. Po zresetowaniu hasła użytkownika przez administratora system musi wymagać od użytkownika zdefiniowania nowego hasła przy pierwszym logowaniu.
10. EZD musi umożliwiać swobodne definiowanie polityki uwierzytelniania i blokowania kont w oparciu o następujące parametry:
    1) Minimalna długość nazwy użytkownika i hasła
    2) Ilość dużych liter, cyfr, znaków specjalnych w haśle,
    3) Długość cyklu wymuszania zmiany hasła (w miesiącach),
    4) Ilość nieudanych prób logowania, po których następuje blokada konta,
    5) Czas blokady konta po przekroczeniu liczby nieudanych prób logowania.
11. Zakres wartości w słownikach prowadzonych przez system powinien być konfigurowalny przez administratora lub pochodzić z rejestrów centralnych (np. TERYT).

12. System w przypadku rejestrów centralnych powinien umożliwiać wyłączenie walidacji pól, które wykorzystują dany rejestr (np. TERYT i pola adresowe), tak by użytkownik mógł dane wprowadzić samodzielnie.
13. EZD musi rejestrować wszystkie czynności dostępu do usług i zasobów w systemie, w tym informacje o:
    1) operacjach na dokumentach,
    2) operacjach na danych osobowych,
    3) zmianach haseł,
    4) zdarzeniach uwierzytelniania (udane logowanie, wylogowanie, nieudane logowanie);
    5) zdarzeniach autoryzacji (nieudane/udane operacje);
    6) zdarzeniach administracyjnych.
14. Zapisywanie danych identyfikujących musi obejmować:
    1) adres IP i nazwę maszyny, z której wykonano daną czynność;
    2) identyfikator/nazwa użytkownika, który wykonał daną czynność;
    3) czas wystąpienia.
    4) EZD musi posiadać mechanizm informujący użytkownika o wprowadzonych zmianach w aplikacji.

Integracja Systemu z Systemami Dziedzinowymi

1. Rozwiązanie musi umożliwiać jednoczesną integrację z dowolną liczbą wdrażanych w ramach niniejszego postępowania Systemów Dziedzinowych (SD).
2. Integracja musi umożliwiać zarówno pobieranie danych z EZD przez SD jak i wysyłanie danych do EZD przez SD.
3. W ramach weryfikacji przez EZD praw SD do wymiany danych, każdorazowe uruchomienie usług przez system kliencki musi wymuszać autoryzację i autentykację SD.
4. W przypadku jednoczesnego serwowania usług dla kilku SD, dane wymieniane z jednym SD nie mogą się mieszać, kolidować i być wspólne z danymi wymienianymi z innymi SD.
5. Dane szczegółowe obiektów udostępnianych przez aplikację w ramach integracji muszą być zawsze dostępne, niezależnie od tego, czy kiedykolwiek wcześniej zostały pobrane, tak aby można je było pobrać dowolną liczbę razy.
6. Zakres wymienianych danych między EZD a SD musi obejmować co najmniej:
    1) dokumenty, sprawy i pliki składające się na dokumenty,
    2) odbieranie i kierowanie dokumentów do wysyłki.
7. Musi istnieć możliwość odmiennej konfiguracji usługi dla kilku różnych SD jednocześnie zintegrowanych z EZD, a zakres tej konfiguracji musi umożliwiać udostępnienie usługi w pełnym lub częściowym zakresie, tj. konfiguracja ma dotyczyć co najmniej:
    1) typów wymienianych dokumentów i spraw,
    2) przyjmowania informacji o danych typach dokumentów,
    3) udzielania informacji o danych typach dokumentów,
    4) przyjmowania zleceń i realizowania wysyłki dokumentów (przesyłek wychodzących).
    5) Aplikacja w ramach usługi musi na każde żądanie SD udostępniać informacje o bieżącej konfiguracji usługi i zakresie wymienianych informacji.
    6) Udostępniana przez aplikację usługa musi umożliwiać realizację wymiany

informacji co najmniej
zgodnie i w zakresie przedstawionym w poniższych wariantach:

Wariant 1:

a) Dokument wpływa do urzędu i jest rejestrowany jako przesyłka przychodząca w EZD, otrzymując numer wpływu.
b) W EZD użytkownik wszczyna sprawę na podstawie dokumentu, nadając jej znak.
c) SD pobiera informacje o dokumencie i sprawie zarejestrowanych w EZD.
d) SD generuje dokument odpowiedzi.
e) SD przekazuje do EZD dokument odpowiedzi (wraz ze składającymi się nań plikami) i dołącza go do sprawy w Systemie EZD.

Wariant 2

a) SD wszczyna postępowanie „z urzędu".
b) SD wprowadza do EZD sprawę wszczętą „z urzędu".
c) SD generuje masowo dokumenty.
d) SD przekazuje do EZD wygenerowane dokumenty i dołącza je do uprzednio wprowadzonej sprawy w EZD.
e) SD wysyła za pośrednictwem Systemu EZD dokumenty do wskazanych adresatów.

Wariant 3

a) Pismo wpływa do urzędu i jest rejestrowane jako przesyłka przychodząca w EZD, otrzymując numer wpływu.
b) SD pobiera informacje o piśmie zarejestrowanym w EZD.
c) SD w EZD dołącza pismo do sprawy już istniejącej w EZD.
d) SD przekazuje do EZD dokument odpowiedzi i dołącza go do sprawy w EZD.

8. Ponadto, integracja musi umożliwiać realizację innych scenariuszy, w których będą występować różne kombinacje zdarzeń opisanych w w/w wariantach.

INSTRUKTAŻ PRACOWNIKÓW

SZBI

1. Użytkownikami systemu będą wszyscy pracownicy Zamawiającego, stąd należy przyjąć, że instruktaże muszą objąć 24 osoby z podziałem na instruktaż dla kancelarii, administratorów i pracowników merytorycznych. Jeżeli ze względu na funkcjonalności systemu konieczne jest wydzielenie dodatkowych grup (np. kierownicy itp.) musi to zostać uwzględnione w ofercie przez Wykonawcę.
2. Zamawiający oczekuje realizacji instruktażu w godzinach pracy jednostki z podziałem pozwalającym na zachowanie ciągłości pracy, co oznacza, że instruktaż dla pracowników merytorycznych winien odbyć się z podziałem minimum na dwie grupy, w różnych terminach.
3. Wymiar czasowy instruktaży musi być adekwatny do zakresu zadań realizowanych we wdrażanych rozwiązaniach przez każdego pracownika i powinien zostać oszacowany przez Wykonawcę w taki sposób, aby każdy pracownik mógł po wdrożeniu sprawnie korzystać z Systemu. Ponieważ zakres obowiązków użytkowników poszczególnych modułów oprogramowania jest zbliżony w różnych urzędach samorządu
szczebla gminnego, oszacowanie wymiaru czasowego instruktaży jest obowiązkiem Wykonawcy, posiadającego w tym zakresie stosowne doświadczenie.

4. Instruktaż należy zaplanować w dwóch turach obejmujących wszystkich pracowników Zamawiającego w każdej turze. Pierwsza i druga tura ma być zrealizowana w trybie stacjonarnym, na podstawie ustalonego z Zamawiającym harmonogramu.
5. Niezależnie od instruktażu Wykonawca zapewni asystę uruchomieniową realizowaną przy stanowiskach pracy wszystkich użytkowników systemu w miarę ich potrzeb. Maksymalny wymiar asysty uruchomieniowej to 2h dla każdego pracownika, przy czym Zamawiający ma prawo zróżnicować czas asysty dla poszczególnych pracowników wg własnych potrzeb (łączny czas asysty wynosi 48h).
6. Niezależnie od instruktażu oraz asysty uruchomieniowej Wykonawca zapewni możliwość skorzystania z nielimitowanego wsparcia w trybie zdalnym (helpdesk/telefon) w całym okresie objętym wsparciem.

AUDYT POSTĘPOWANIA Z DOKUMENTACJĄ, SZKOLENIE Z PRZEPISÓW PRAWA, WSPARCIE MERYTORYCZNE

1. Wykonawca w ramach wdrożenia przeprowadzi audyt postępowania z dokumentacją.
2. Zakres audytu obejmie zarządzenia i procedury wewnętrzne, związane z wykonywaniem przez Zamawiającego czynności kancelaryjnych na różnych etapach pracy z dokumentacją oraz próbki dokumentów wytwarzanych i gromadzonych przez Zamawiającego.
3. Zamawiający przekaże Wykonawcy zarządzenia, instrukcje, procedury oraz skany zanonimizowanych dokumentów. Ilość i zakres przekazanych materiałów do audytu zostanie ustalony z Wykonawcą.
4. Po przekazaniu Zamawiającemu wyników audytu, Wykonawca przeprowadzi dla pracowników Zamawiającego szkolenie online dotyczące przygotowania urzędu do wdrożenia systemu
5. Szkolenie będzie trwało minimum 6 godzin (z przerwami ustalonymi z Zamawiającym) w godzinach pracy jednostki. Będzie omówieniem zasad postępowania z dokumentacją zgodnie z obowiązującymi u Zamawiającego: regulaminem organizacyjnym, instrukcją kancelaryjną, jednolitym rzeczowym wykazem akt, wybranymi zagadnieniami Kodeksu postępowania administracyjnego oraz z uwzględnieniem tematów, które po przeprowadzonym audycie będą wymagały szczególnej uwagi. Szkolenie, oprócz zagadnień formalnych, będzie zawierało tematy praktyczne i organizacyjne, związane z wdrożeniem systemu EZD i będzie okazją do rozmowy i odpowiedzi na pytania pracowników Zamawiającego. Szkolenie będzie nagrywane i wraz z materiałami szkoleniowymi udostępnione Zamawiającemu do późniejszego wykorzystania.
6. Audyt i szkolenie Wykonawca powinien zrealizować przed instruktażami pracowników z obsługi funkcjonalności systemu. Zamawiający wymaga takiej kolejność działań, ponieważ oczekuje, że audyt i szkolenie przyczynią się do sprawdzenia i powtórzenia podstawowych zasad postępowania z dokumentacją oraz umożliwią Zamawiającemu podjęcie różnych decyzji organizacyjnych, zanim pracownicy przejdą instruktaż z obsługi systemu.
7. Wykonawca zapewni pracownikom Zamawiającego wsparcie merytoryczne w zakresie konsultacji stosowania przepisów prawa, dotyczących postępowania z dokumentacją. Wsparcie będzie realizowane przez okres 24 miesięcy, liczony od dnia następnego po podpisaniu przez obie strony protokołu odbioru

końcowego w wymiarze 48 godzin miesięcznie. Konsultacje będą realizowane telefonicznie, online oraz poprzez korespondencję e-mail na zasadach ustalonych z Wykonawcą.

OGÓLNE WARUNKI GWARANCJI

1. Świadczenie usługi gwarancji w okresie 24 miesięcy rozpocznie swój bieg:
   1) w dniu następnym, licząc od daty potwierdzenia usunięcia wad lub usterek stwierdzonych przy odbiorze końcowym przedmiotu umowy,
   2) w dniu następnym, licząc od dnia podpisania przez obie strony protokołu odbioru końcowego, w przypadku gdy nie stwierdzono wad lub usterek,
2. W przypadku, jeżeli Wykonawca dokona modernizacji istniejącego systemu informatycznego, zmodernizowany system informatyczny musi zostać objęty gwarancją na warunkach określonych w niniejszym rozdziale. Świadczenie usługi gwarancji ma na celu zapewnienie ciągłości sprawnego działania systemu poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych błędów i wad systemów, niewłaściwego działania systemu, spadku wydajności oraz zmian prawnych uniemożliwiających zgodne z prawem funkcjonowanie systemu
3. W ramach gwarancji Wykonawca zobowiązany jest do nieodpłatnego:
   1) aktualizacji systemu do najnowszych wersji,
   2) usuwania błędu, awarii, wady z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: błędu w systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę;
   3) usuwania błędu, awarii, wady związanych z realizacją usługi wdrożenia oprogramowania;
   4) usuwania błędów lub awarii spowodowanych aktualizacjami oprogramowania.
4. Zgłaszający, w przypadku wystąpienia błędu, awarii, wady przesyła do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia błędu/awarii/wad
5. Zgłoszenia będą klasyfikowane na awarie, błędy i wady:
   1) Awaria - krytycznie wadliwa praca systemu lub jego części, niezgodna z przekazaną dokumentacją lub warunkami Umowy, polegająca na zatrzymaniu lub zakłóceniu pracy systemu lub jego części w takim zakresie, że nie istnieje możliwość realizacji przez Zamawiającego istotnych dla jego organizacji procesów (na przykład: niedostępne są usługi dla mieszkańców będące celem zamówienia, czy też niemożliwe jest terminowe wypełnienia przez Zamawiającego obowiązków wynikających z przepisów wewnętrznych lub zewnętrznych) lub też nieprawidłowość pracy części systemu w takim zakresie, że kontynuowanie jego działania doprowadziłoby do utraty danych lub naruszenia ich spójności, w przypadku Awarii nie jest możliwe prawidłowe użytkowanie systemu z powodu w szczególności uszkodzenia lub utraty spójności danych, struktur danych lub błędnego funkcjonowania platformy systemowo-sprzętowej;
   2) Błąd - wadliwa praca Systemu lub jego części, niezgodna z przekazaną dokumentacją lub warunkami Umowy, polegająca na zakłóceniu pracy Systemu lub jego części innym niż Awaria.;
   3) Wada - wadliwa praca Systemu lub jego części polegające na

nienależytym działaniu jego części,
nieograniczająca działania Systemu, nie mająca istotnego wpływu na zastosowanie Systemu.

6. Wykonawca zobowiązany jest do usunięcia awarii/błędów/wad występujących w oprogramowaniu aplikacyjnym lub infrastrukturze kluczowej w następujących terminach:
   1) Awarie w terminie nie dłuższym niż 8h roboczych od przyjęcia zgłoszenia przez Wykonawcę.
   2) Błędy w terminie nie dłuższym niż 3 dni roboczych od przyjęcia zgłoszenia przez Wykonawcę,
   3) Wady w terminie nie dłuższym niż 10 dni roboczych od przyjęcia zgłoszenia przez Wykonawcę.
7. W przypadku niemożności usunięcia awarii, błędu lub wady w terminie, o którym mowa w ust. 6 Wykonawca jest zobowiązany pisemnie uzasadnić zwłokę i wskazać termin usunięcia danej awarii, błędu lub wady. W takim przypadku Zamawiający zastrzega sobie prawo w uzasadnionych przypadkach do pisemnej odmowy akceptacji terminu podanego przez Wykonawcę i skorzystania z uprawnień zawartych w ust. 8.
8. W przypadku niespełnienia zobowiązań określonych w ust. 6 i 7 względnie odmowy akceptacji podanego terminu usunięcia danej awarii, błędu lub wady zgodnie z ust. 7, Zamawiający może zlecić wykonanie napraw osobie trzeciej na koszt Wykonawcy – bez konieczności wyznaczania dodatkowego terminu i upoważnienia sądu.
9. Wykonawca ponosi wobec Zamawiającego odpowiedzialność za wyrządzone szkody, będące normalnym następstwem nienależytego wykonania czynności objętych umową, ocenianego w granicach przewidzianych przez Kodeks cywilny.
10. Wszystkie reklamacje dotyczące niepełnego, nienależytego lub nieterminowego wykonania przedmiotu umowy, Zamawiający będzie przekazywał niezwłocznie Wykonawcy w formie pisemnej.
11. Usługobiorca wyznacza osoby odpowiedzialne za merytoryczną obsługę EZD (administratorów technicznych).
12. Administrator lub inna osoba do tego upoważniona zgłasza problem dotyczący działania systemu do Usługodawcy. Każde zgłoszenie otrzyma unikalny numer, na podstawie którego będzie prowadzona dalsza komunikacja w sprawie zgłoszenia.

4. Dodatkowe wymagania.

System musi umożliwiać integrację z systemem dziedzinowym SIGID w zakresie wymiany danych. Integracja stanowi element przedmiotu zamówienia i podlega realizacji przez Wykonawcę. Okres gwarancji na system wynosi minimum 24 miesiące i obejmuje wsparcie techniczne oraz aktualizacje.

Wykonawca zobowiązany jest do wykonania pełnej instalacji, konfiguracji oraz uruchomienia Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji, w tym wdrożenia wszystkich modułów systemu, dostosowania ich parametrów do środowiska Zamawiającego oraz integracji z istniejącą infrastrukturą teleinformatyczną Zamawiającego. W ramach realizacji zamówienia Wykonawca przeprowadzi szkolenia dla administratorów i użytkowników systemu.

System musi umożliwiać integrację z systemami zewnętrznymi administracji publicznej, w szczególności z Krajowym Systemem e-Faktur (KSeF) oraz systemem e-Doręczeń. Wykonawca zobowiązany jest do wykonania konfiguracji, uruchomienia oraz przetestowania tych integracji zgodnie z obowiązującymi standardami komunikacyjnymi oraz wymaganiami technicznymi właściwych operatorów systemów.

Wszelkie integracje systemu z systemami zewnętrznymi oraz systemami Zamawiającego realizowane są w całości przez Wykonawcę. Wykonawca ponosi odpowiedzialność za ich konfigurację, uruchomienie, przetestowanie oraz zapewnienie ich poprawnego działania. Realizacja integracji nie może wymagać od Zamawiającego zakupu dodatkowych komponentów, licencji ani usług podmiotów trzecich, chyba że zostało to jednoznacznie wskazane w ofercie i zaakceptowane przez Zamawiającego przed zawarciem umowy.

Warunkiem uznania przedmiotu zamówienia za należycie wykonany jest podpisanie przez Strony protokołu odbioru końcowego bez zastrzeżeń. Odbiór zostanie poprzedzony testami funkcjonalnymi i integracyjnymi przeprowadzonymi w środowisku Zamawiającego.