SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (SOPZ)

1. Spis treści

2. Spis tabel

3. Spis rysunków

4. Wprowadzenie

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia na Audyt bezpieczeństwa kodu i aplikacji.

Tło Projektu ZSI-ULC opisane zostało w rozdziale 6 oraz w rozdziale 9.

5. Słownik pojęć i skrótów

Tabela 1. Terminy i skróty ogólne

Termin	Objaśnienie
CPPC	Centrum Projektów Polska Cyfrowa
Dzień roboczy	Dzień kalendarzowy od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych.
EASA	Z ang. *European Aviation Safety Agency* - Europejska Agencja Bezpieczeństwa Lotniczego - jeden z instytucjonalnych filarów europejskiego systemu bezpieczeństwa lotniczego obok Komisji Europejskiej, organizacji EUROCONTROL oraz krajowych władz lotniczych. Została powołana do życia na mocy rozporządzenia Rady i Parlamentu Europejskiego nr 1592/2002 i rozpoczęła swoją działalność we wrześniu 2003 roku. Obecnie podstawą prawną jej funkcjonowania jest rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 216/2008 z dnia 20 lutego 2008 r. w sprawie wspólnych zasad w zakresie lotnictwa cywilnego i utworzenia Europejskiej Agencji Bezpieczeństwa Lotniczego oraz uchylające dyrektywę Rady 91/670/EWG, rozporządzenie (WE) nr 1592/2002 i dyrektywę 2004/36/WE (Dz. U. L 79 z 19.3.2008).
EFRR	Europejski Fundusz Rozwoju Regionalnego - fundusz utworzony w 1975 r. na podstawie art. 160 Traktatu ustanawiającego Wspólnotę Europejską. Zgodnie z tym przepisem, celem funduszu jest „przyczynianie się do korygowania podstawowych dysproporcji regionalnych we Wspólnocie poprzez niwelowanie różnic w poziomach rozwoju oraz zacofania regionów".
Godzina robocza/Roboczogodzina	Okres trwający godzinę zegarową w ramach godziny pracy Zamawiającego.
Godziny pracy Zamawiającego	Od 8:15 do 16:15, od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
Inżynier Kontraktu/Doradca	Firma Avility Sp. z o. o. realizująca Umowę na „Świadczenie usługi konsultanta zewnętrznego - usługi doradcze Inżyniera Kontraktu w ramach realizacji Projektu pod nazwą „Doskonalenie i rozbudowa Zintegrowanego Systemu Informatycznego ZSI-ULC".
Kod źródłowy	Słowniki, skrypty, definicje, pliki źródłowe bazy danych, jak również biblioteki, algorytmy oraz jakiekolwiek inne

	symboliczne lub konwencjonalne przedstawienie zapisu informacji, niezbędne do kompilacji, wykonania i utrzymania, funkcjonowania i utrzymania Systemu, z wyłączeniem Oprogramowania standardowego.
Narzędzie do rejestracji i obsługi zgłoszeń	Narzędzie do rejestracji i zarządzania zgłoszeniami (z ang. *Issue Tracking Systems*), który pozwala na przyjmowania zgłoszeń, kategoryzację incydentów, nadawanie im priorytetu, delegowanie do odpowiednich osób, monitorowanie statusu zgłoszenia i śledzenia historii jego realizacji.
POPC	Program Operacyjny Polska Cyfrowa
Porozumienie o dofinansowanie	Porozumienie nr POPC.02.02.00-00-0010/17-00 o dofinansowanie Projektu „Doskonalenie i rozbudowa Zintegrowanego Systemu Informatycznego ZSI-ULC" w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa nr 2 „E-administracja i otwarty rząd", Działanie nr 2.2 „Cyfryzacja procesów back-office w administracji rządowej" pomiędzy CPPC, a ULC.
Prawo Lotnicze	Ustawa z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz.U. z 2020 r. poz. 1970).
PRINCE2	Z ang. *Project IN Controlled Environment* – ustrukturyzowana metodyka zarządzania projektami bazująca na doświadczeniach Kierowników Projektów, zespołów projektowych, a także szkoleniowców i konsultantów. PRINCE2 przedstawia zarządzanie projektem jako cztery zintegrowane elementy – pryncypia, tematy, procesy i środowisko projektu.
Procedura	Ustalona metoda postępowania obejmująca tryb i sposób prowadzenia spraw według określonych kroków. Procedury realizowane przez Pracowników Urzędu Lotnictwa Cywilnego zamodelowane zostały jako procesy biznesowe.
Projekt/ZSI-ULC/Projekt ZSI-ULC	Projekt „Doskonalenie i rozbudowa Zintegrowanego Systemu Informatycznego ZSI-ULC" w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa nr 2 „E-administracja i otwarty rząd", Działanie nr 2.2 „Cyfryzacja procesów back-office w administracji rządowej".
Przedmiot Zamówienia	Zobowiązanie Wykonawcy wynikające z niniejszego SOPZ i SIWZ.
SOA	Z ang. *Service-oriented architecture* - architektura zorientowana na usługi - koncepcja tworzenia systemów informatycznych, w której główny nacisk stawia się na definiowanie usług, które spełnią wymagania użytkownika. SOA obejmuje zestaw metod organizacyjnych i technicznych mający na celu powiązanie biznesowej strony organizacji z jej zasobami informatycznymi.
SOPZ	Szczegółowy Opis Przedmiotu Zamówienia
System	Budowany w ramach Projektu System ZSI-ULC.

Środowisko uruchomieniowe	Oprogramowanie, które stanowi platformę w rozumieniu infrastruktury oprogramowania dla oprogramowania rozwiązania, tożsame z pojęciem z ang. *execution environment* ze specyfikacji UML.
TOGAF	Metodyka i szkielet do budowy aplikacji dla architektury korporacyjnej. Właścicielem standardu jest konsorcjum The Open Group.
ULC/Urząd/Beneficjent/Zamawiający	Urząd Lotnictwa Cywilnego
Umowa	Umowa pomiędzy Wykonawcą a Zamawiającym, obejmująca realizację zadań wynikających z niniejszej dokumentacji, w szczególności wynikającej z rozdziału 8
UX/User Experience	Z ang. *User Experience* – całość wrażeń, które doświadcza użytkownik podczas korzystania z produktu interaktywnego. Projektowanie User Experience polega na projektowaniu produktów interaktywnych w taki sposób, aby interakcja z nimi powodowała w użytkownikach pozytywne emocje.
WCAG 2.1	Z ang. *Web Content Accessibility Guidelines* – wytyczne dla dostępności treści internetowych 2.1.
Wykonawca Audytu Bezpieczeństwa Kodów i Aplikacji/Wykonawca Audytu	Podmiot wybrany w drodze oddzielnego postępowania, realizujący Umowę na przeprowadzenie Audytu Bezpieczeństwa Kodu w ramach realizacji Projektu pod nazwą „Doskonalenie i rozbudowa Zintegrowanego Systemu Informatycznego ZSI-ULC”.
Wykonawca/Główny Wykonawca Systemu/Wykonawca Systemu	Podmiot wybrany w drodze jednego z wcześniejszych postępowań, realizujący Umowę na Wytworzenie oprogramowania Systemu ZSI-ULC.
Wykonawcy zewnętrzni	Podmioty realizujące oddzielne umowy w ramach realizacji Projektu pod nazwą „Doskonalenie i rozbudowa Zintegrowanego Systemu Informatycznego ZSI-ULC”.
Wymagania biznesowe	Wymagania określające cele i wymagane rezultaty.
Wymaganie funkcjonalne	Wymagania opisujące możliwości, jakie dane rozwiązanie musi posiadać pod względem zachowania oraz informacji, jakimi dane rozwiązanie będzie zarządzać.
Wymagania rozwiązania	Wymagania opisujące możliwości i cechy rozwiązania, które spełniają wymagania interesariuszy. Wymagania zapewniają odpowiedni poziom szczegółowości umożliwiający opracowanie i wdrożenie rozwiązania. Wyróżnia się podział wymagań rozwiązania na wymagania funkcjonalne, pozafunkcjonalne i przejściowe.
Wymaganie pozafunkcjonalne/niefunkcjonalne	Wymagania dotyczące jakości usług, nie odnoszące się bezpośrednio do zachowania funkcjonalności rozwiązania, lecz opisujące warunki, w których to rozwiązanie musi pozostać pod względem przydatności funkcjonalnej, wydajności, kompatybilności, użyteczności, niezawodności, bezpieczeństwa, utrzymania i przenoszenia.

6. Kontekst realizacji zamówienia oraz ogólne informacje o Projekcie ZSI-ULC

Przedmiotem Projektu jest informatyzacja obszaru back-office Urzędu Lotnictwa Cywilnego w zakresie działalności realizowanej przez ULC. Głównym celem Projektu jest usprawnienie funkcjonowania działalności ULC poprzez cyfryzację procesów i procedur dotyczących funkcjonowania obszaru back-office. Odbędzie się to m.in. poprzez wdrożenie rozwiązań umożliwiających obsługę niezinformatyzowanych obszarów działalności Urzędu. Projekt zakłada uruchomienie lub modernizację następujących modułów funkcjonalnych, które będą się składały na Zintegrowany System Informatyczny ULC:

- Moduł Obsługi Personelu Lotniczego,
- Moduł Techniki Lotniczej,
- Moduł Obsługi Operacji Lotniczych,
- Moduł Zarządzania Bezpieczeństwem w Lotnictwie Cywilnym,
- Moduł Rejestru Lotnisk i Lądowisk,
- Moduł Obsługi Ochrony Praw Pasażerów,
- Moduł Ochrony i Ułatwień w Lotnictwie Cywilnym,
- Moduł Zarządzania Rynkiem Transportu Lotniczego,
- Moduł Żeglugi Powietrznej,
- Moduł Zarządzania Urzędem.

Wdrożenie powyższych modułów oraz uruchomienie ZSI-ULC wynika ze zidentyfikowanych problemów i potrzeb, jakie występują w codziennej działalności Urzędu oraz kierowanych przez Klientów i instytucji współpracujących z ULC.

Najważniejszymi interesariuszami Projektu będą wszyscy pracownicy ULC, klienci i podmioty zewnętrzne mające potrzeby załatwiania spraw w ULC oraz organizacje nadzoru lotnictwa (międzynarodowe i europejskie).

W ramach Projektu zostaną także przeszkoleni użytkownicy (pracownicy ULC) w zakresie m.in obsługi nowego Systemu, a administratorzy uzyskają odpowiednie kwalifikacje do administrowania i utrzymania efektów Projektu. Zakłada się, że po zakończeniu realizacji Projektu działania realizowane w Urzędzie będą odbywały się z wykorzystaniem ZSI-ULC, co zaowocuje efektywniejszym wykonywaniem obowiązków oraz realizacją spraw wynikających z obowiązków ustawowych Beneficjenta dla zidentyfikowanych odbiorców Projektu.

Projekt ZSI-ULC realizowany jest w ramach Porozumienia nr POPC.02.02.00-00-0010/17-00 o dofinansowanie Projektu „Doskonalenie i rozbudowa Zintegrowanego Systemu Informatycznego ZSI-ULC" pomiędzy CPPC a ULC, Program Operacyjny Polska Cyfrowa na lata 2014-2020 Oś Priorytetowa nr 2 „E-administracja i otwarty rząd" Działanie nr 2.2 „Cyfryzacja procesów back-office w administracji rządowej" (3 konkurs) i jako taki podlega regulacjom i zasadom niniejszego konkursu, Programu Operacyjnego Polska Cyfrowa oraz zapisom ww. porozumienia.

W ramach realizacji Projektu ZSI-ULC, oprócz zamówienia stanowiącego przedmiot niniejszego postępowania, realizowane są następujące umowy:

- Świadczenie usługi konsultanta zewnętrznego - usługi doradcze Inżyniera Kontraktu.
- Promocja.
- Dostawa infrastruktury sprzętowej wraz z oprogramowaniem systemowym.
- System ZSI-ULC.

7. Miejsce realizacji

Miejscem realizacji Przedmiotu Zamówienia jest siedziba Urzędu Lotnictwa Cywilnego w Warszawie, ul. Marcina Flisa 2, 02-247 Warszawa.

8. Przedmiot Zamówienia

Przedmiotem Zamówienia jest przeprowadzenie Audytu bezpieczeństwa kodu i aplikacji Zintegrowanego Systemu Informatycznego ZSI-ULC. Audyt obejmować będzie spełnienie przez Głównego Wykonawcę Systemu ZSI-ULC wymagań pozafunkcjonalnych dotyczących bezpieczeństwa Systemu oraz bezpieczeństwa przetwarzanych w nim danych.

W ramach Przedmiotu Zamówienia Wykonawca Audytu zobowiązany jest do wykonania poniższych Zadań:

a) audyt bezpieczeństwa Systemu,
b) testy penetracyjne Systemu,
c) audyt Kodu źródłowego,
d) ocena końcowa bezpieczeństwa Systemu,
e) ocena bezpieczeństwa przetwarzania danych osobowych.

Celem audytu jest wykrycie faktycznych oraz potencjalnych podatności i luk Systemu oraz jego Kodu źródłowego wraz z identyfikacją błędów konfiguracji i błędów programowych, które mogą być

wykorzystane do naruszenia bezpieczeństwa przetwarzanych informacji, a także bezpieczeństwa Zamawiającego lub Użytkowników Systemu. Przeprowadzenie audytu na etapie wytwarzania i przekazywania do użytkowania Systemu pozwolić ma na dostarczenie odbiorcom projektu rozwiązań gwarantujących osiągnięcie wymaganego poziomu bezpieczeństwa w fazie użytkowania.

Wykonawca po wykonaniu audytów i testów przedstawi raporty, które zawierać będą m.in. przyjęte założenia badawcze i uzasadnienie wyboru technik i metod badania, dokumentację wykonanych prac, wyniki wraz z ich interpretacją, identyfikację niezgodności z wymaganiami i założeniami oraz luk i błędów Systemu, analizę wyników oraz rekomendacje dotyczące usunięcia niezgodności oraz luk i błędów Systemu, a także rekomendacje dotyczące poprawy bezpieczeństwa Systemu, zmian w architekturze oraz Kodzie źródłowym, ze szczególnym uwzględnieniem punktu widzenia potrzeb dalszego jego utrzymania oraz rozwoju, uwzględniając najlepsze praktyki stosowane przy wytwarzaniu, utrzymaniu, rozwoju oraz dokumentowaniu systemów informatycznych.

Audyt bezpieczeństwa Systemu, testy penetracyjne Systemu oraz audyt Kodu źródłowego obejmują wykonanie po jednym re-teście/re-audycie w ramach realizacji Przedmiotu Zamówienia, po dokonaniu przez Wykonawcę zmian w Systemie na podstawie rekomendacji przedstawionych w raportach poaudytowych i potestowym. Ponowne audyty i testy oznaczają weryfikację wszystkich podatności wymienionych w danym raporcie.

Podsumowaniem prac będzie Raport końcowy bezpieczeństwa Systemu oraz Raport bezpieczeństwa przetwarzania danych osobowych. Wyniki ponownych audytów oraz testów zostaną uwzględnione w ocenie końcowej bezpieczeństwa Systemu i ujęte w obydwu raportach końcowych. Raport końcowy bezpieczeństwa Systemu będzie zawierał identyfikację i ocenę długu technologicznego wraz z rekomendacjami.

8.1 Zakres prac

1) W ramach Zamówienia, Wykonawca Audytu będzie zobowiązany do świadczenia usług polegających na wykonywaniu Zadań wskazanych w Przedmiocie Zamówienia w zakresie bezpieczeństwa Systemu i przetwarzanych w nim danych, w tym ich poufności, integralności, dostępności, autentyczności, rozliczalności, niezaprzeczalności oraz niezawodności.
2) Zakres prac będzie obejmował analizę i ocenę realizacji przez Wykonawcę Systemu wymagań w zakresie bezpieczeństwa, zleconych Wykonawcy Systemu w ramach Projektu ZSI-ULC.
3) Audyty bezpieczeństwa Systemu oraz Kodu źródłowego obejmować będą co najmniej:
   a) określenie powierzchni ataku,
   b) określenie obszarów podwyższonego ryzyka,

c) określenie zgodności ze standardami organizacji,

d) identyfikacja klas podatności.

4) Ocena bezpieczeństwa Systemu oraz Kodu źródłowego z perspektywy podatności na ataki obejmować będzie co najmniej:

a) weryfikacja metod uwierzytelniania i autoryzacji,

b) weryfikacja metod dostępu do baz danych,

c) weryfikacja procesu logowania,

d) weryfikacja istnienia backdoorów,

e) weryfikacja wykorzystania zewnętrznych bibliotek (i ich wersji) pod kątem użycia podatnych (niebezpiecznych lub niewspieranych) wersji bibliotek,

f) weryfikacji kodu na możliwość przeprowadzenia ataków z uwzględnieniem metodologii OWASP.

5) Zakres audytu Kodu źródłowego będzie obejmować co najmniej:

a) audyt podatności na ataki (co najmniej SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), ataki Man-In-The-Middle, ataki na hasła),

b) audyt jakości wykonanych testów automatycznych (zasięg i pokrycie),

c) audyt obecności oraz jakości komentarzy umieszczonych w Kodzie źródłowym,

d) audyt czytelności i wydajności Kodu źródłowego,

e) audyt optymalizacji oraz normalizacji baz danych,

f) audyt poprawności wykorzystania framework'ów,

g) audyt kosztów modyfikacji podczas utrzymania i rozwoju Systemu.

6) Wykonawca wykona analizę statyczną i analizę powtórzeń Kodu źródłowego, wraz ze wskazaniem obszarów ryzyka oraz nieoptymalnych formuł stosowanych w przypadku poszczególnego języka programowania i/lub stosowanego framework'u.

7) Testy penetracyjne Systemu ZSI-ULC zostaną zrealizowane poprzez określenie faktycznego stanu bezpieczeństwa polegające na symulacji prób złamania lub ominięcia zabezpieczeń. W trakcie testów zastosowane będą metody i narzędzia, którymi zwykle posługują się potencjalni napastnicy. Zidentyfikowane podatności są wykorzystywane do przejęcia kontroli nad testowanymi systemami oraz do dalszych prób eskalacji ataku. Umożliwia to określenie potencjalnej skali naruszenia bezpieczeństwa, która wystąpi, jeśli te podatności zostaną wykorzystane przez hackerów. Testy obejmować będą następujące obszary:

a) testy penetracyjne serwera WWW,

b) testy penetracyjne serwera aplikacyjnego,

c) testy penetracyjne aplikacji (komponenty dostępne publicznie),

d) testy penetracyjne aplikacji (po uwierzytelnieniu),

e) testy penetracyjne interfejsów bazy danych,

f) testy penetracyjne bazy danych z poziomu użytkownika.

Realizacja Przedmiotu Zamówienia obejmuje wykonanie testów automatycznych, oznaczających identyfikację podatności występujących w Systemie i jego Kodzie źródłowym przy pomocy automatycznych narzędzi testujących.

8) W ramach testów penetracyjnych zostaną wykorzystane dwa rodzaje testów:
   a) black box (z minimalną wiedzą o audytowanym Systemie),
   b) crystal box (z pełną wiedzą i kontem użytkownika w audytowanym Systemie).
9) Audytom oraz testom penetracyjnym podlegać będzie System ZSI-ULC funkcjonujący w określonym środowisku Zamawiającego.
10) Testy penetracyjne Systemu będą przeprowadzane na instancjach przeznaczonych do testowania (nieprodukcyjnych).
11) Prace będą realizowane na środowiskach wskazanych przez Zamawiającego.
12) Prace mogą wymagać obecności Wykonawcy w siedzibie Zamawiającego.

8.2 Oprogramowanie wymagane do realizacji umowy

Ze względu na złożoność Systemu, który zostanie poddany Audytowi bezpieczeństwa, Zamawiający wymaga, w celu osiągnięcia kompletności analizy, przeprowadzenia badania za pomocą automatycznego skanera klasy Static Application Security Testing oraz testów manualnych.

Oferent musi posiadać potwierdzone kompetencje w zakresie użytkowania oprogramowania, które zostanie użyte podczas audytu, co najmniej na poziomie Silver lub równoważnym. Potwierdzenie kompetencji musi być wystawione przez producenta rozwiązania bądź autoryzowany przez producenta ośrodek certyfikacyjny.

Wymagania dotyczące oprogramowania:

1. Oprogramowanie musi obsługiwać analizę statyczną kodu.
2. Oprogramowanie musi umożliwiać analizę kodu źródłowego dla co najmniej następujących technologii: Java, Swift, Spring, Angular, mikroserwisy, konteneryzacja.
3. Oprogramowanie musi posiadać możliwość wykrywania martwego kodu.

4. Oprogramowanie musi posiadać możliwość wykrywania potencjalnych problemów wydajnościowych w analizowanym kodzie źródłowym.
5. Oprogramowanie musi posiadać możliwość filtrowania wyników analizy ze względu na język programowania, kategorię, ryzyko znalezionego problemu.
6. Oprogramowanie musi posiadać możliwość konfigurowania kryteriów analizy kodu źródłowego.
7. Oprogramowanie musi posiadać możliwość skanowania kodu źródłowego z lokalnych repozytoriów GIT.
8. Oprogramowanie musi pokazywać użytkownikowi szczegółowy opis wykrytej podatności, a także sposób jej naprawy.
9. Oprogramowanie musi posiadać możliwość określenia standardów rozwijania oprogramowania oraz sprawdzania, czy rozwijane oprogramowanie postępuje zgodnie z nimi poprzez wykresy i powiadomienia.
10. Oprogramowanie musi posiadać możliwość prezentacji zbiorczej wykrytych błędów na wykresach i dashboardach.
11. Oprogramowanie musi mieć możliwość automatycznego wskazania linii w kodzie poprzez wyszczególnienie tych, które zawierają błędy bezpieczeństwa.
12. Oprogramowanie musi nadawać poziom krytyczności dla każdej znalezionej podatności.
13. Oprogramowanie musi informować użytkownika o postępach skanowania.
14. Oprogramowanie musi działać w oparciu o algorytmy analizy przepływu danych, to znaczy rozpatrywać zasięg i czas życia zmiennych oraz zależności pomiędzy nimi.
15. Oprogramowanie musi działać w oparciu o identyfikację zmiennych kontrolowanych przez użytkownika oraz analizować w jakich funkcjach są one wykorzystywane w celu określenia bezpieczeństwa funkcji korzystających z tych zmiennych.
16. Narzędzie musi pozwalać na analizowanie kodu aplikacji pod kątem występowania podatności, w tym podatności występujących na listach OWASP TOP 10 i CWE TOP 25.
17. Narzędzie musi posiadać funkcjonalność lokalnego serwera proxy pozwalającą na kontrolę i analizę ruchu HTTP/HTTPS przesyłanego pomiędzy przeglądarką testera a serwerem WWW testowanej aplikacji.
18. Narzędzie musi posiadać możliwość nagrywania i analizy ruchu (wysłanych zapytań i odpowiedzi aplikacji), zbierania próbki standardowej funkcjonalności aplikacji i tworzenia nowych zapytań na podstawie wcześniej zebranej próbki.

19. Narzędzie musi posiadań możliwość nagrywania sesji testowych, oraz modyfikacji i odtwarzania sesji testowych.
20. Narzędzie musi posiadań wsparcie dla automatycznej enumeracji zasobów, wysyłania żądań, oraz wspierać ocenę praktycznej entropii losowych wartości, w tym dla np. ciasteczek, tokenów, identyfikatorów obiektów.
21. Narzędzie musi posiadać wbudowaną funkcjonalność raportową pozwalającą na generowanie raportów z przeprowadzonych testów bezpieczeństwa.
22. Oprogramowanie powinno umożliwiać generowanie raportów bezpieczeństwa
23. Oprogramowanie musi priorytetyzować i kategoryzować znalezione podatności.
24. Oprogramowanie musi wspierać możliwość uruchomienia skanowania zarówno z poziomu wiersza poleceń, jak i z poziomu interfejsu graficznego (GUI).
25. Oprogramowanie musi wykrywać co najmniej 900 kategorii podatności.
26. Oprogramowanie musi pozwalać na grupowanie podatności wedle najpopularniejszych standardów, co najmniej OWASP, SANS, CWE i FISMA.
27. Oprogramowanie musi być rozpoznawane jako lider w magicznym kwadracie firmy analitycznej Gartner.
28. Oprogramowanie musi posiadać możliwość uruchamiania skanowania dynamicznego za pomocą REST API.
29. Oprogramowanie musi umożliwiać skanowanie aplikacji Web, a także webserwisów REST i SOAP.
30. Oprogramowanie musi pozwalać na skanowanie aplikacji SPA.
31. Oprogramowanie musi posiadać skonfigurowane polityki i raporty dla głównych regulacji zgodności, w tym co najmniej PCI DSS, DISA STIG, NIST 800-53, ISO 27K, OWASP i HIPPAA.

9. System ZSI ULC

Projekt ZSI-ULC jest odpowiedzią na zapotrzebowanie zgłaszane ze strony klientów oraz innych współpracujących z ULC podmiotów gospodarczych i agend rządowych Polski, UE – EASA i światowych - ICAO. Działalność ULC jest związana z realizacją procesów m.in. w następujących obszarach:

- Personel Lotniczy,
- Technika Lotnicza,
- Operacje Lotnicze,
- Bezpieczeństwo w Lotnictwie Cywilnym,

- Lotniska,
- Ochrona Praw Pasażerów,
- Ochrona w Lotnictwie Cywilnym,
- Rynek Transportu Lotniczego,
- Żegluga Powietrzna,
- Zarządzanie Urzędem.

W ramach procesów realizowanych przez ULC w ramach działań ustawowych, gromadzone, przechowywane i przetwarzane są dane dotyczące całej działalności Urzędu, w tym dane osób lub firm związanych z działalnością lotniczą oraz dane medyczne personelu lotniczego. Wszystkie procesy, poza procesami związanymi z Personelem Lotniczym (głównie w zakresie przeprowadzania egzaminów i licencjonowania) są realizowane z wykorzystaniem rozproszonych zbiorów, często powielających dane. Do pracy wykorzystywane jest głównie oprogramowanie MS Office (Word i Excel). Obecnie tylko niewielki odsetek przetwarzanych dokumentów posiada formę elektroniczną (ok. 1,5%). Pracownicy ULC w 10 z 12 obszarów działalności ULC (poza obszarami: Współpraca międzynarodowa i europejska oraz Obsługa prawno-legislacyjna), zgłaszają potrzebę wdrożenia rozwiązań usprawniających obsługę swoich zadań, co wynika również z oczekiwań Klientów Urzędu.

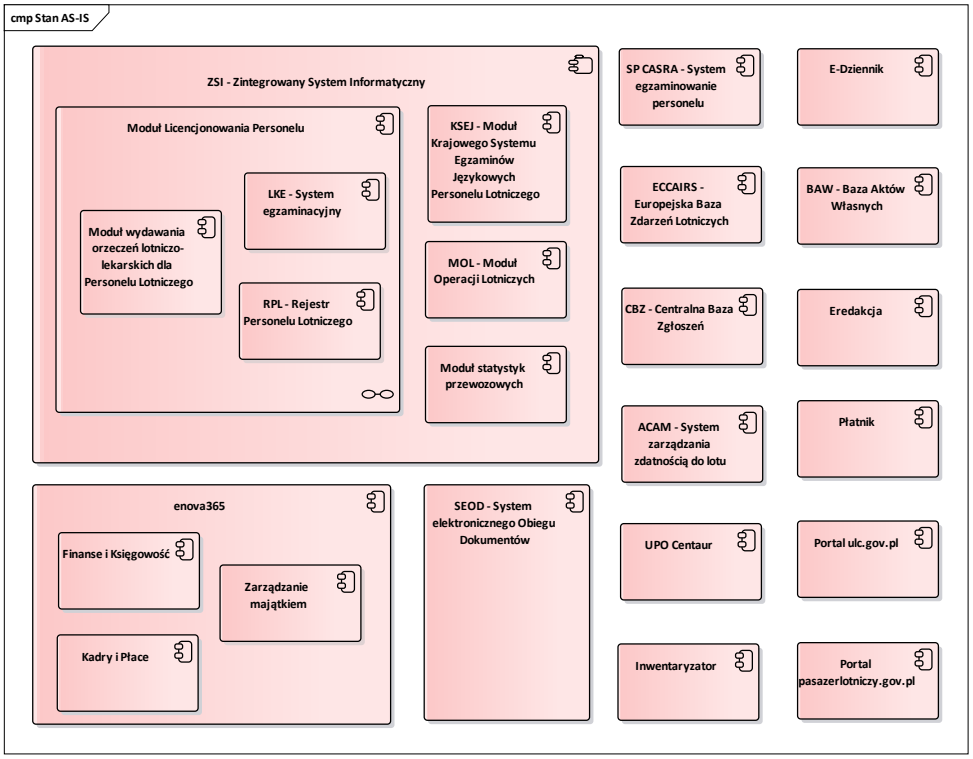
Obecnie systemy informatyczne eksploatowane przez ULC wspierają głownie realizację procesów związanych z zarządzaniem i obsługą Personelu Lotniczego. Główne elementy istniejącego systemu informatycznego eksploatowanego przez ULC to:

- Zintegrowany System Informatyczny (ZSI) składający się z:
    - Modułu wydawania orzeczeń lotniczo-lekarskich dla Personelu Lotniczego,
    - Rejestru Personelu Lotniczego (RPL),
    - Systemu egzaminacyjnego (LKE),
    - Modułu Krajowego Systemu Egzaminów Językowych Personelu Lotniczego,
    - Modułu Operacji Lotniczych,
    - Modułu statystyk przewozowych.
- System Elektronicznego Obiegu Dokumentów (SEOD);
- System wspomagania zasobami Urzędu (enova365) składający się modułów:
    - Finanse i Księgowość,
    - Kadry i Płace,
    - Zarządzanie Majątkiem.
- System egzaminowania personelu (SP CASRA),

- Europejska Baza Zdarzeń Lotniczych (ECCAIRS),
- Centralna Baza Zgłoszeń (CBZ),
- System zarządzania zdatnością do lotu (ACAM).

W ramach Projektu przewiduje się budowę nowego Systemu ZSI-ULC. System ZSI-ULC będzie zintegrowany z obecnym Systemem wspomagania zasobami Urzędu (enova365), a jego funkcjonalności obejmą funkcjonalności obecnego Systemu Elektronicznego Obiegu Dokumentów (SEOD) oraz Systemu zarządzania zdatnością do lotu (ACAM).

Obecna architektura systemów w sposób poglądowy została przedstawiona na poniższym rysunku.



Rysunek 1 Architektura obecnych systemów ULC

9.1 Wykorzystana technologia

Warstwę klienta stanowi aplikacja frontend w technologii HTML i frameworku Javascript – Angular 8. Layout stron oparty został na bibliotece arkuszy styli CSS – Bootstrap. Do implementacji wykorzystany został szablon Metronic.

Aplikacja frontend, po pobraniu do przeglądarki użytkownika, komunikuje się z API systemu, wystawionym jako usługi REST z komunikatami w formacie JSON.

Warstwą pośredniczącą w komunikacji systemu ZSI-ULC z systemami zewnętrznymi oraz wystawianiu usług poza ekosystem ZSI-ULC jest komponent - szyna danych w rozwiązaniu WSO2 Enterprise Integrator 7 w wersji Community.

Backend systemu zaimplementowany został w języku programowania Java 11. Za środowisko uruchomieniowe posłużył OpenJDK od RedHat, który jest wersją niekomercyjną. Aplikacje implementowane są przy wykorzystaniu frameworka developerskiego Spring 5.X. Za warstwę ORM posłużyła biblioteka Hibernate.

Asynchroniczna komunikacja między komponentami w backendzie odbywa się po protokole JMS, który jest standardem i ma wbudowane API w języku java.

Procesy biznesowe obsługi spraw, realizowane w systemie, zaimplementowane są w silniku procesów biznesowych Activiti w notacji BPMN.

Do przechowywania danych w systenie wykorzystana została baza danych Postgresql 12.X.

Autentykacja i uprawnienia w systemie oparte zostaną na dedykowanym rozwiązaniu IAM. Podstawą tego komponentu będzie WSO2 Identity Server.

Cały backend systemu uruchomiony został na platformie konteneryzacyjnej OKD.

9.2 Wielkość Systemu

Poniżej przedstawiono wielkość (w liniach kodu) Systemu ZSI-ULC. Z uwagi na to, że wciąż trwają prace nad Systemem poniższe dane należy traktować jako orientacyjne.

Język	Liczba plików	Ilość linii kodu
TypeScript	1 351	65 455
Java	1 435	41 749
SQL	416	41 517
HTML	365	39 061
SASS	283	31 878
JSON	25	16 703
Javascript	32	4 844
Maven	29	3 835
CSS	8	2 307
YAML	38	1 488
XML	6	911

9.3 Harmonogram prac nad Systemem ZSI-ULC

Poniżej wskazane zostały planowane kluczowe daty związane z pracami developerskimi nad Systemem ZSI-ULC:

- Grudzień 2020 r. - Wdrożenie modułów funkcjonalnych Systemu,
- Grudzień 2020 r. - Przeprowadzenie testów akceptacyjnych oprogramowania ZSI-ULC,
- Styczeń 2021 r. - Odbiór zainstalowanej infrastruktury sprzętowo-programowej,
- Marzec 2021 r. - Odbiór oprogramowania ZSI,
- Kwiecień 2021 r. - Odbiór końcowy wdrożenia.

9.4 Licencje

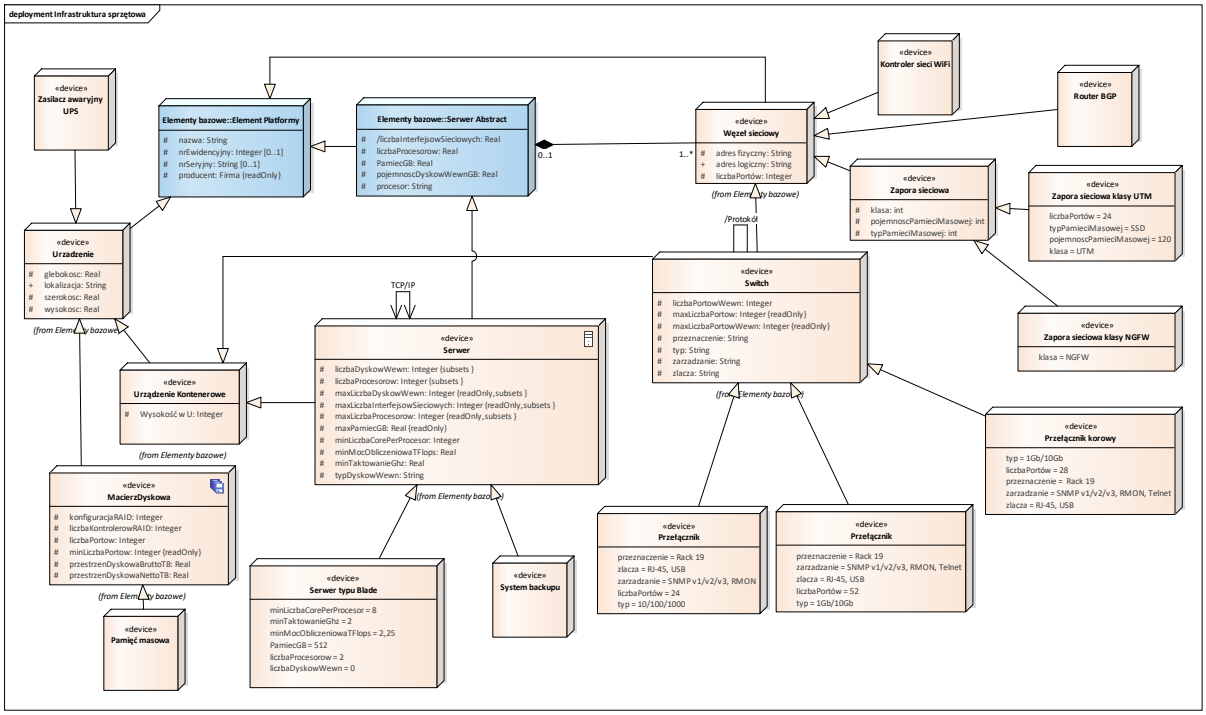
Biblioteka	Licencja
Java 11	GNU General Public License
Spring	Apache License 2.0
Angular 8	MIT License
Bootstrap	MIT License
WSO2 EI	Apache License 2.0
PostgreSQL	PostgreSQL License
Jasper Reports Server	GNU Affero General Public License version 3
Elasticsearch	Apache License 2.0
Hibernate	LGPL 2.1
Activiti	Apache License 2.0
OKD	Apache License 2.0
Gradle	Apache License 2.0
NPM	Artistic License 2.0

10. Infrastruktura

10.1 Infrastruktura sprzętowa przeznaczona do budowy Systemu ZSI-ULC

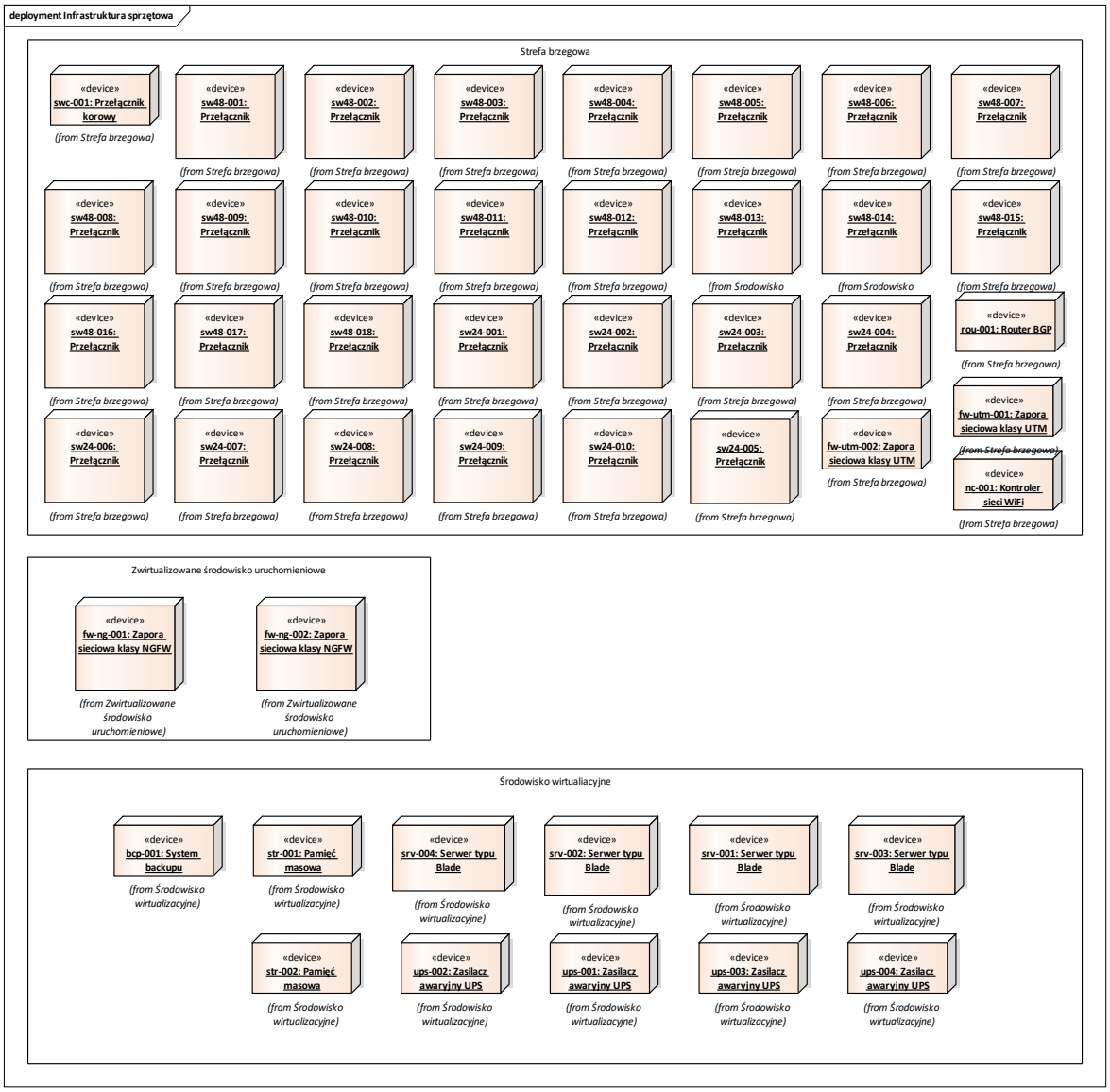
System ZSI-ULC zostanie zbudowany bazując na rozwiązaniu tzw. chmury prywatnej (ang. Private cloud) utworzonej na potrzeby wewnętrzne Urzędu, w modelu zgodnym z IaaS (ang. Infrastructure as

a Service). Model chmury obliczeniowej zakłada, że zasoby obliczeniowe będące w posiadaniu ZSI-ULC udostępniane będą w ramach zwirtualizowanego środowiska (VMware) i będą dostępne jedynie w sieci wewnętrznej Urzędu. Zwirtualizowane środowisko ZSI-ULC będzie wykorzystywało infrastrukturę sprzętową ZSI-ULC (dostarczoną w ramach odrębnego zamówienia). Docelowa infrastruktura przeznaczona przez Zamawiającego na realizację ZSI-ULC obejmuje klasy urządzeń zgodne z Rysunkiem 2 Klasy urządzeń przeznaczone do budowy Systemu ZSI-ULC.



Rysunek 2 Klasy urządzeń przeznaczone do budowy Systemu ZSI-ULC

Liczba poszczególnych urządzeń udostępnionych przez Zamawiającego na potrzeby budowy ZSI-ULC (dostarczonych w ramach oddzielnego postępowania) będzie zgodna z modelem zaprezentowanym na Rysunku 3 Instancje urządzeń przeznaczone do budowy Systemu ZSI-ULC.



Rysunek 3 Instancje urządzeń przeznaczone do budowy Systemu ZSI-ULC

10.2 Środowiska programistyczne

W ramach realizacji Projektu ZSI-ULC planuje się wykorzystanie poniższych środowisk dedykowanych tworzeniu i testowaniu nowych funkcjonalności:

- Środowisko developerskie (DEV) - środowisko deweloperskie Wykonawcy służące do przeprowadzenia testów wewnętrznych (w tym testów jednostkowych). Za środowisko odpowiada w całości Wykonawca.
- Środowisko testowe (TEST) - środowisko testowe Wykonawcy służące do testowania nowych funkcjonalności oraz funkcjonalności po poprawkach błędów. Środowisko będzie

wykorzystywane do przeprowadzania testów wewnętrznych oraz ewentualnych testów akceptacyjnych (funkcjonalnych). Za środowisko odpowiada w całości Wykonawca.

- Środowisko przedprodukcyjne (PRE_PROD) - środowisko przedprodukcyjne Systemu ZSI-ULC rozmieszczone i skonfigurowane przez Wykonawcę na infrastrukturze technicznej Zamawiającego (dostarczonej w ramach oddzielnego postępowania). Środowisko to stanowi po wdrożeniu podstawę do odbioru Systemu w ramach przeprowadzenia testów akceptacyjnych (funkcjonalnych i jakościowych).
- Środowisko produkcyjne (PROD) - środowisko produkcyjne Systemu ZSI-ULC rozmieszczone na infrastrukturze technicznej Zamawiającego (tożsamej ze środowiskiem PRE_PROD).
- Środowisko testowe służące rozwojowi (TEST_ROZWOJ) - Środowisko testowe przeznaczone na rozwój Systemu ZSI-ULC rozmieszczone i skonfigurowane przez Wykonawcę na infrastrukturze technicznej Zamawiającego (dostarczonej w ramach oddzielnego postępowania).

11. Wymagane Produkty podlegające odbiorowi

Niniejszy rozdział zawiera zestawienie Produktów wymaganych do wytworzenia i dostarczenia celem sfinalizowania przez Wykonawcę Audytu Przedmiotu Zamówienia. Liczba dni na weryfikację Zamawiającego określona została w dniach roboczych.

Tabela 2. Lista Produktów specjalistycznych podlegających odbiorowi

Lp.	Produkt	Typ Produktu	Liczba dni na I weryfikację Zamawiającego	Liczba dni na II weryfikację Zamawiającego
1	Audyt bezpieczeństwa Systemu	Dokument	7	3
2	Audyt Kodu źródłowego	Dokument	7	3
3	Testy penetracyjne Systemu ZSI-ULC	Dokument	7	3
4	Raport końcowy bezpieczeństwa Systemu	Dokument	7	3
5	Raport bezpieczeństwa przetwarzania danych osobowych	Dokument	7	3

12. Terminy realizacji prac

Przedmiot Zamówienia zostanie wykonany w terminie nie dłuższym niż 2 miesiące od dnia udostępnienia przez Zamawiającego zasobów infrastruktury sprzętowej oraz Systemu.

13. Procedury odbioru

Wszystkie Produkty wskazane w rozdziale 11 stanowiące efekt realizacji Przedmiotu Zamówienia podlegają weryfikacji i oficjalnym procedurom odbioru.

Wzory Protokołów Przekazania oraz Odbiorów zawarto w załącznikach do Umowy.

13.1 Odbiór Produktów

Niniejszej procedurze odbioru podlegają Produkty, które w rozdziale 11. Wymagane Produkty podlegające odbiorowi zostaną poddane weryfikacji przez Zamawiającego, zgodnie z procedurą opisaną poniżej:

1. Wykonawca przekazuje Produkt do odbioru Zamawiającemu wraz z Protokołem Przekazania Produktu.
2. Zamawiający weryfikuje dostarczony Produkt w czasie nie dłuższym niż termin wskazany dla Produktu w Rozdziale 11.
3. Jeśli Zamawiający nie zgłasza uwag, to następuje podpisanie Protokołu Odbioru Produktu i zakończenie procedury odbioru. W przeciwnym wypadku Zamawiający rejestruje uwagi, które są przekazywane Wykonawcy za pośrednictwem **Narzędzia do rejestracji i obsługi zgłoszeń**.
4. W uzgodnionym z Zamawiającym terminie Wykonawca może zorganizować spotkanie w celu omówienia uwag Zamawiającego. Organizacja spotkania nie wydłuża terminu oddania poprawionej wersji Produktu.
5. Wykonawca przekazuje w uzgodnionym terminie poprawiony o wskazane przez Zamawiającego uwagi Produkt do odbioru Zamawiającego. Wykonawca zobowiązany jest przekazać razem z poprawionym Produktem odniesienia do zgłoszonych uwag zawierające informacje dotyczące sposobu, w jaki zostały one obsłużone. Zaktualizowana dokumentacja musi zostać dostarczona w taki sposób, aby widoczne były w nim naniesione zmiany (np. w trybie „śledzenia zmian”).
6. Jeżeli Zamawiający ponownie zgłosi uwagi do Produktu następuje przejście procedury do kroku „4”. Jeżeli Produkt spełnia wymogi odbioru (mieści się w limitach błędów określonych dla tego typu Projektu) następuje podpisanie Protokołu Odbioru Produktu i procedura odbioru zostaje zakończona.

13.2 Odbiór Przedmiotu Zamówienia

Procedura Odbioru Przedmiotu Zamówienia będzie rozpoczęta wyłącznie w sytuacji, w której wszystkie produkty wskazane do realizacji w ramach przedmiotu zamówienia zostały pozytywnie odebrane. Procedura odbioru Przedmiotu Zamówienia przebiega następująco:

1. Wykonawca przedkłada Zamawiającemu Protokół Odbioru Przedmiotu Zamówienia.
2. W przypadku akceptacji realizacji Przedmiotu Zamówienia podpisywany jest Protokół Odbioru Przedmiotu Zamówienia.

14. Zobowiązania Wykonawcy

W ramach realizacji Przedmiotu Zamówienia Wykonawca zobowiązany jest do przestrzegania i realizacji poniższych zasad.

1. Przedmiot Zamówienia musi zostać zrealizowany przez Wykonawcę z najwyższą starannością, efektywnością oraz zgodnie z najlepszą praktyką i wiedzą zawodową.
2. Całość Przedmiotu Zamówienia musi zostać zrealizowana zgodnie z terminem określonym w Rozdziale 12.
3. Wykonawca jest zobowiązany do dokonywania wszelkich niezbędnych ustaleń mogących wpływać na Przedmiot Zamówienia z Zamawiającym.
4. Wykonawca sprawnie i terminowo zrealizuje Przedmiot Zamówienia, w tym uwzględni w trakcie jego realizacji wszystkie uwagi zgłaszane przez Zamawiającego.
5. Wykonawca będzie współpracował z powołanym przez Zamawiającego zespołem projektowym dedykowanym do realizacji Projektu po stronie Zamawiającego.
6. Wykonawca udzieli Zamawiającemu wszelkich informacji na temat stanu realizacji Przedmiotu Zamówienia.
7. Wykonawca jest zobowiązany do stałego kontaktu z Zamawiającym (spotkania przedstawicieli Wykonawcy i Zamawiającego będą odbywać się odpowiednio do potrzeb w siedzibie Zamawiającego), z następującymi maksymalnymi czasami reakcji ze strony Wykonawcy na wezwanie Zamawiającego:
    a. spotkanie w siedzibie Zamawiającego – do 3 dni roboczych od zgłoszenia konieczności, przez Zamawiającego, nie częściej niż 4 razy w miesiącu;

b. telekonferencja, kontakt online – do 2 dni roboczych od zgłoszenia konieczności, przez Zamawiającego, (poprzez kanał telekonferencyjny, czat, oprogramowanie do wideokonferencji);
c. kontakt email – do 6 godzin roboczych od zgłoszenia konieczności przez Zamawiającego;
d. kontakt telefoniczny – niezwłocznie, tj. maksymalnie do 4 godzin roboczych od zgłoszenia konieczności przez Zamawiającego;

8. Po każdorazowym spotkaniu Wykonawca sporządzi notatkę i przekaże ją stronom spotkania maksymalnie do 1 dnia roboczego po spotkaniu. Zamawiający w terminie 3 dni roboczych zgłasza ewentualne uwagi do notatki. Wykonawca wprowadza wskazane uwagi w terminie 2 dni roboczych. Notatka musi być zaakceptowana i podpisana przez obydwie strony.
9. Wykonawca będzie współpracował z Zamawiającym, Głównym Wykonawcą Systemu ZSI-ULC oraz Inżynierem Kontraktu na każdym etapie wykonywania Przedmiotu Zamówienia w ramach realizacji Umowy w celu zapewnienia wypełnienia wskaźników Produktu i rezultatu Projektu ZSI-ULC.

15. Zobowiązania Zamawiającego

Zamawiający w ramach realizacji przez Wykonawcę Przedmiotu Zamówienia zobowiązany jest do:

1. Udostępnienia wszelkich materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, które są niezbędne celem realizacji Przedmiotu Zamówienia.
2. Informowania Wykonawcy o wszelkich czynnościach, którą mogą mieć wpływ na realizację Przedmiotu Zamówienia przez Wykonawcę.
3. Udostepnienia obiektów, sprzętu, Oprogramowania i Dokumentacji, które są niezbędne do realizacji Przedmiotu Zamówienia zgodnie z polityką bezpieczeństwa i regulacjami wewnętrznymi, obowiązującymi Zamawiającego.
4. Udostępnienia niezbędnej do realizacji przedmiotu zamówienia infrastruktury technicznej.