OPIS PRZEDMIOTU ZAMÓWIENIA zmieniony V.2
(Zasady i zakres świadczenia usługi Utrzymania i Rozwoju Systemu)

dla postępowania o udzielenie zamówienia publicznego prowadzonego pod nazwą:
„Usługi utrzymania i rozwoju systemu Rejestracji i Ewidencji Firm Audytorskich STREFA PANA"

(znak spr. 1/2023/PZP)

prowadzonego przez Polską Agencję Nadzoru Audytowego,
w trybie przetargu nieograniczonego na podstawie na podstawie art. 3 ust. 1 pkt 1
Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych
(Dz.U. z 2022 roku poz. 1710 ze zm.)

I. Zasady i zakres świadczenia usługi Utrzymania Systemu

1. Udzielanie wsparcia administratorom Systemu:

   1.1. Zakres usług obejmuje udzielanie wsparcia administratorów Systemu, w Dni robocze w godzinach 08:00-17:00, obejmującego m.in. wykonanie i pomoc przy instalacji i konfiguracji Systemu, a w szczególności:

      1.1.1. tworzenie backupu i procedur backupowych oraz awaryjnego przywracania Systemu;

      1.1.2. optymalizację baz danych;

      1.1.3. podnoszenie wersji środowiska i konfigurację, również na serwerach wirtualnych;

      1.1.4. analiza logów;

      1.1.5. monitorowanie i optymalizacja miejsca na infrastrukturze Systemu;

      1.1.6. doradztwo architektoniczne w zakresie zgodności sposobu wykorzystywania technologii wykorzystywanych w Systemie z najlepszymi praktykami rynkowymi oraz zgodności z warunkami Utrzymania Systemu;

      1.1.7. przegląd wydajności Systemu pod kątem identyfikacji zagrożeń skalowania lub wydłużenia czasów reakcji na poziomie konfiguracji sprzętowo-systemowej, konfiguracji oraz na poziomie konstrukcji eksploatowanego Systemu;

      1.1.8. przegląd konfiguracji Systemu pod kątem zgodności z warunkami Utrzymania Systemu, stabilności pracy oraz wysokiej dostępności;

      1.1.9. wykonywanie zmian konfiguracji Systemu w celu zachowania jego stabilnej wydajności.

   1.2. Zamawiający przekazuje Wykonawcy Zgłoszenie potrzeby wsparcia administratorów Systemu przez 24 godziny na dobę 7 dni w tygodniu za pośrednictwem jednego z kanałów komunikacji, z zastrzeżeniem że obsługa Zgłoszenia następuje w godzinach świadczenia usługi wskazanych w pkt. 1.1. powyżej:

      1.2.1. poczty elektronicznej na adres ..... (rejestracja Zgłoszenia w systemie Service Desk po stronie Wykonawcy);

1.2.2. aplikacji Service Desk, udostępnianej przez Wykonawcę, za pośrednictwem formatki ekranowej zgłoszenia;

1.2.3. w przypadku konieczności realizacji wsparcia administratorów systemu w siedzibie Zamawiającego – także telefonicznie w godzinach świadczenia usługi wskazanych w pkt 1.1. powyżej (rejestracja Zgłoszenia w systemie Service Desk po stronie Wykonawcy).

1.3. Czas realizacji Zgłoszenia potrzeby wsparcia administratorów Systemu:

1.3.1. wykonawca udziela wsparcia administratorom Systemu nie później niż w następnym Dniu roboczym;

1.3.2. w wyjątkowych przypadkach Zamawiający może wydłużyć termin udzielenia wsparcia o dodatkowe 24 godziny. Informacja o przedłużeniu terminu zostanie przekazana przez Zamawiającego pisemnie bądź za pośrednictwem poczty elektronicznej.

2. Rozpoznawanie przyczyn i usuwanie Błędów oraz skutków błędów.

2.1. Rozpoznawanie przyczyn i usuwanie Błędów oraz skutków Błędów, rozpoznawanie skutków Awarii, a także wszelkich negatywnych skutków spowodowanych korzystaniem z błędnie działających zmodyfikowanych wersji Systemu, mające na celu przywrócenie pełnej funkcjonalności i wydajności Systemu obejmuje:

2.1.1. analizę szczegółową zgłoszenia i diagnozę przyczyn wystąpienia problemu;

2.1.2. opracowanie zmiany w oprogramowaniu polegającej na przygotowaniu poprawki usuwającej zgłoszony Błąd;

2.1.3. przeprowadzenie testów jednostkowych przygotowanej poprawki/zmiany na środowisku pomocniczym i po pozytywnym wyniku przekazanie poprawki wraz z raportem z testów;

2.1.4. przekazanie zmiany w oprogramowaniu w postaci kodów źródłowych wraz z opisem zmiany i dodatkowymi informacjami dot. specyfiki danej modyfikacji oraz instrukcją jej instalacji.

2.2. Kategorie Błędów i czas realizacji Zgłoszeń:

Zamawiający stawia minimalne wymagania w zakresie czasu realizacji zgłoszeń, zgodnie z tabelą:

Kategoria	Opis	Priorytet	Maksymalny czas realizacji
Awaria	stan w funkcjonowaniu Systemu powodujący brak możliwości uruchomienia lub całkowite unieruchomienie Systemu lub brak dostępu Odbiorcy usług lub Odbiorców Usług do Systemu lub brak dostępu Użytkowników zewnętrznych do Systemu.	Krytyczny	do **4,5 godzin** zegarowych od Zgłoszenia przez Zamawiającego lub Użytkownika albo stwierdzenia Awarii przez Wykonawcę, liczonych w oknie 8:00-17:00, 5 dni w tygodniu (poniedziałek -piątek)
Błąd	nieprawidłowe działanie	Wysoki	do **18 godzin**

krytyczny	Systemu powodujące albo całkowity brak możliwości korzystania z Systemu albo takie ograniczenie możliwości korzystania z niego, że przestaje ono spełniać swoje podstawowe funkcje, w szczególności niemożność uruchomienia Oprogramowania, brak odczytu/zapisu z bazy danych, utrata danych lub ich spójności, brak możliwości zalogowania użytkownika, niedostępność krytycznych funkcji Systemu		zegarowych od Zgłoszenia przez Zamawiającego lub Użytkownika albo stwierdzenia Błędu krytycznego przez Wykonawcę, liczonych w oknie 8.00-17.00, 5 dni roboczych w tygodniu
Błąd zwykły	nieprawidłowe działanie Systemu powodujące ograniczenie korzystania z niego, przy zachowaniu spełniania jego podstawowych funkcji, w szczególności niedostępność niekrytycznych funkcji Systemu	Średni	do **50 godzin** zegarowych od Zgłoszenia przez Zamawiającego lub Użytkownika albo stwierdzenia Błędu zwykłego przez Wykonawcę, liczonych w oknie 8.00-17.00, 5 dni roboczych w tygodniu
Błąd drobny	nieprawidłowe działanie Systemu niepowodujące ograniczenia korzystania z jego funkcji, w szczególności Błędem drobnym jest niedostępność systemu pomocy, błąd językowy w interfejsie	Niski	do **100 godzin** zegarowych od Zgłoszenia przez Zamawiającego lub Użytkownika albo stwierdzenia Błędu drobnego przez Wykonawcę, liczonych w oknie 8.00-17.00, 5 dni roboczych w tygodniu

2.3. Zgłaszanie potrzeby usunięcia Błędu lub Awarii:

2.3.1. Zamawiający zgłasza Wykonawcy Błędy za pośrednictwem jednego z kanałów komunikacji:

2.3.1.1. poczty elektronicznej ..... (rejestracja Zgłoszenia w systemie Service Desk po stronie Wykonawcy),

2.3.1.2. aplikacji Service Desk, udostępnionej przez Wykonawcę, za pośrednictwem formatki ekranowej zgłoszenia.

2.3.2. Zamawiający zgłasza Wykonawcy Błędy w Dni robocze w godzinach 08:00 – 17:00. Zgłoszenie przesłane przez Zamawiającego po godz. 17:00 w dniu

roboczym Wykonawca przyjmuje do realizacji następnego Dnia roboczego o godz. 08:00.

2.3.3. Wykonawca informuje z zachowaniem formy pisemnej lub elektronicznej na bieżąco Zamawiającego o wszelkich zmianach adresu poczty elektronicznej dedykowanego wyłącznie do obsługi zgłoszeń serwisowych, co najmniej 14 Dni roboczych przed zmianą. Zmiana danych, o którym mowa powyżej, nie wymaga zmiany Umowy.

2.3.4. Zamawiający określa domyślny kanał komunikacji do zgłaszania usługi oraz będzie miał możliwość zmiany kanału komunikacji po wcześniejszym 7 dniowym uprzedzeniu Wykonawcy. Zamawiający zastrzega miał możliwość zmiany formatki ekranowej nie więcej niż raz na kwartał.

2.3.5. W przypadku kanału:

2.3.5.1. poczty elektronicznej Wykonawca potwierdza w 1 Dzień roboczy przyjęcie zgłoszenia,

2.3.5.2. w przypadku kanału Service Desk wskazanie Wykonawcy do realizacji zgłoszenia jest równoważne z potwierdzeniem przez Wykonawcę przyjęcia zgłoszenia do realizacji.

2.4. Procedura realizacji usług i ich odbiór:

2.4.1. Zamawiający kategoryzuje zgłoszenia wskazując rodzaj Błędu zgodnie z kwalifikacją określoną w tabeli – Kategorie Błędów i Czas Zgłoszeń.

2.4.2. Wykonawca potwierdza przyjęcie zgłoszenia do realizacji, przesyłając zwrotnie potwierdzenie przyjęcia zgłoszenia tym samym kanałem komunikacji.

2.4.3. W przypadku zgłoszenia w aplikacji Service Desk, godzina (HH:MM) przekazania zlecenia Wykonawcy traktowana jest jako godzina przyjęcia zgłoszenia do realizacji.

2.4.4. Wykonawca po wykonaniu naprawy zgłasza System do odbioru przesyłając odpowiednią informację do Zamawiającego pocztą elektroniczną lub w systemie Service Desk. Data przekazania (yyyy-mm-dd hh:mm) jest uznawana za zakończenie zgłoszenia pod warunkiem potwierdzenia realizacji zgłoszenia przez zgłaszającego usługę.

2.4.5. W przypadku zgłoszenia przez Wykonawcę prośby o uszczegółowienie zgłoszenia, czas dostarczenia dodatkowej informacji przez Zamawiającego nie wlicza się do czasu realizacji zgłoszenia.

2.5. Ewidencja zgłoszeń Awarii i Błędów:

2.5.1. Wykonawca prowadzi w systemie Service Desk ewidencję zgłoszeń zawierającą minimum:

2.5.1.1. identyfikator awarii lub błędu,

2.5.1.2. datę i godzinę zgłoszenia w formacie yyyy-mm-dd hh:mm, gdzie: yyyy- określa rok, mm- określa miesiąc, dd- określa dzień miesiąca, hh- określ godzinę w danym dniu, mm- określa minutę w godzinie,

2.5.1.3. datę i godzina przyjęcia zgłoszenia przez Wykonawcę (yyyy-mm-dd hh:mm),

2.5.1.4. rodzaj Błędu lub Awarii,

2.5.1.5. określenie zgłaszającego wraz z numerem telefonu kontaktowego i poczty elektronicznej,

2.5.1.6. nazwę komponentu lub funkcjonalności Systemu którego dotyczy problem,

2.5.1.7. opis Awarii lub Błędu (treść merytoryczna zgłoszenia),

2.5.1.8. imię i nazwisko osoby rozwiązującej zgłoszenie,

2.5.1.9. datę i godzinę rozwiązania zgłoszenia (w formacie yyyy-mm-dd hh:mm),

2.5.1.10. sposób rozwiązania zgłoszenia,

2.5.1.11. opis zmian wprowadzonych do bazy danych,

2.5.1.12. aktualizację dokumentacji technicznej i użytkowanej Systemu, o ile uległa zmianie,

2.5.1.13. ewentualne uwagi.

2.6. Miejsce realizacji usługi:

2.6.1. Usunięcie Awarii i Błędu Systemu oraz skutków awarii Systemu, sprzętu i Oprogramowania, a także wszelkich negatywnych skutków spowodowanych korzystaniem z błędnie działających wersji Systemu Wykonawca realizuje zdalnie.

2.6.2. Dla naprawy danych w bazie danych lub modyfikacji bazy danych Wykonawca przygotowuje skrypty naprawcze wraz z odpowiednimi procedurami, które wykonuje Zamawiający, z zastrzeżeniem, że Zamawiający może wskazać Wykonawcę do realizacji tych prac.

3. Monitorowanie konieczności aktualizacji i instalacji poprawek / nowych wersji technologicznych lub nowych rozwiązań technologicznych na środowiskach technologicznych Systemu.

3.1. Zakres usług obejmuje:

3.1.1. monitorowanie konieczności zainstalowania poprawek i nowych wersji na potrzeby Systemu, na poszczególnych elementach Systemu, takich jak:

3.1.1.1. oprogramowanie sieciowych systemów operacyjnych,

3.1.1.2. oprogramowanie aplikacyjne,

3.1.1.3. oprogramowanie bazodanowe,

3.1.1.4. oprogramowanie komunikacyjne (o ile System zawiera tego typu oprogramowanie),

3.1.1.5. oprogramowanie do prezentacji treści,

3.1.1.6. oprogramowanie wirtualizacyjne (w tym w zakresie Disaster Recovery SRM, High Availability w VMware),

3.1.1.7. oprogramowanie do backupu,

3.1.1.8. oprogramowanie do monitorowania działania Systemu;

oraz pozostałego oprogramowania technologicznego i narzędziowego wykorzystywanego w obszarze Systemu.

Wykonawca zobowiązany jest do wskazania, czy rekomenduje konieczność zainstalowania poprawek i nowych wersji.

4. Aktualizacja Dokumentacji w trakcie realizacji zadań związanych ze świadczeniem usługi Utrzymania Systemu obejmuje wykonanie aktualizacji Dokumentacji związanej z realizacją usługi Utrzymania Systemu.
5. Administrowanie usługą publicznej chmury obliczeniowej przeznaczoną dla Systemu oraz Oprogramowaniem gotowym, w tym w szczególności systemami operacyjnymi, serwerami aplikacyjnymi, oprogramowaniem bazodanowym i integracyjnym, w tym również w modelu Software as a Service ***(zmiana dokonana w wyniku odpowiedzi na pytanie nr16)***.

II. Zasady i zakres świadczenia usługi Rozwoju Systemu

1. Rozwój Systemu oraz przygotowanie dokumentów analitycznych i projektów zmian w Systemie obejmuje swoim zakresem:
   1.1. modyfikację Oprogramowania Systemu (w tym rozwój programistyczny Systemu);
   1.2. przeprowadzenie analiz i przygotowanie dokumentów analitycznych i innych dokumentów oraz projektów zmian w Systemie;
   1.3. przygotowanie procedur, instrukcji, standardów, wytycznych w zakresie procesów funkcjonujących w Systemie;
   1.4. wykonanie wraz z Zamawiającym testów akceptacyjnych, których celem będzie potwierdzenie wykonywania w sposób prawidłowy wszystkich funkcjonalności Systemu,
   1.5. opracowanie techniczne w dziedzinie zastosowań technologii lub modyfikacji środowisk, w którym jest ono zastosowane, w zakresie uzgodnionym między Stronami;
   1.6. doradztwo techniczne, implementacja rozwiązań technicznych, wsparcie merytoryczne;
   1.7. doradztwo techniczne, wytworzenie dodatkowych funkcjonalności i wsparcie implementacyjne w zakresie adaptacji nowych i dodatkowych funkcjonalności;
   1.8. doradztwo architektoniczne dla nowych lub dodatkowych funkcjonalności;
   1.9. opracowywanie projektów technicznych wraz z koncepcjami rozwoju;
   1.10. wykonywanie otwartych interfejsów oraz rozwiązań w oparciu o narzędzia / oprogramowanie udostępniane przez Zamawiającego oraz dostosowywanie oraz konfiguracja interfejsów;
   1.11. aktualizację wytworzonych w ramach warsztatów wewnętrznych materiałów dydaktycznych.
2. Wytworzone Oprogramowanie Dedykowane i Dokumentacja przekazywane są przyrostowo w sekwencjach czasowych określonych w założeniach ustalonych pomiędzy Zamawiającym a Wykonawcą, np. raz na miesiąc/kwartał/pół roku/rok/na koniec etapów.

3. Wytworzone Oprogramowanie Dedykowane i Dokumentacja składają się z:
   3.1. produktów analitycznych (np. wyników analiz, projektów architektury),
   3.2. produktów wytwórczych (np. kodów źródłowych, przygotowane testy funkcjonalne, przygotowane testy jednostkowe, przygotowane testy integracji, przygotowane testy wydajnościowe, opracowane scenariusze testowe wraz z raportami wykonania),
   3.3. produktów zamkniętych (np. wykorzystywane oprogramowanie wraz z licencjami wystawionymi na Polską Agencję Nadzoru Audytowego),
   3.4. produktów konfiguracyjnych (np. instrukcje instalacji/konfiguracji na środowisku deweloperskim, testowym i produkcyjnym).
4. Oprogramowanie dedykowane nie może zawierać produktów innych podmiotów, co do których Polska Agencja Nadzoru Audytowego nie posiada licencji albo praw do ich wykorzystania i powielania oraz dalszego użytkowania, w tym bibliotek, komponentów, kodów źródłowych podmiotów trzecich.
5. Po dostarczeniu Oprogramowania Dedykowanego wymagane jest zapewnienie prawa do wykorzystania wszystkich licencji na oprogramowanie i biblioteki wykorzystywane w trakcie kompilacji, testów, instalacji i wdrożenia Oprogramowania oraz jego wykorzystywania. Dostarczone prawa do ww. Produktów i ich składowych muszą obejmować okres do min. 3 lat wraz ze wsparciem producenta od daty dostarczenia danego Produktu.
6. Zasady przeprowadzenia testów akceptacyjnych:
   6.1. Testy akceptacyjne zostaną przeprowadzone na podstawie scenariuszy testowych przygotowanych przez Wykonawcę przed przeprowadzeniem testów akceptacyjnych i zatwierdzonych przez Zamawiającego.
   6.2. Scenariusze testowe służą do określenia zadań wykonywanych przez użytkowników Systemu.
   6.3. Każdy scenariusz testowy powinien być odzwierciedleniem dokładnie określonej funkcjonalności Systemu.
   6.4. Zamawiający oceni prawidłowość działania Systemu stosując 3 kategorie Błędów:
      6.4.1. Błąd krytyczny;
      6.4.2. Błąd zwykły;
      6.4.3. Błąd drobny;

      których znaczenie jest identyczne jak dla usługi Utrzymania Systemu.
   6.5. Znajdowane w trakcie testów Błędy w Systemie będą dokumentowane na przygotowanych przez Wykonawcę do tego celu formularzach, które oprócz danych zawierających: datę wykrycia Błędu, wersję oprogramowania, w której został wykryty, nazwiska osoby, która go znalazła będą zawierały kategorię Błędu wraz z zwięzłym opisem istoty Błędu i opisem czynności wykonanych przez osobę testującą. Zamawiający dopuszcza możliwość elektronicznego dokumentowania procesu testowania.
   6.6. Testy akceptacyjne zostaną zakończone, gdy wszystkie scenariusze testowe zostaną zakończone wynikiem pozytywnym.

7. Zamawiający ma prawo do weryfikacji wdrożonych w Systemie zabezpieczeń, zgodnie z wymaganiami bezpieczeństwa określonymi w pkt III poprzez sprawdzenie wszystkich lub wybranych zabezpieczeń. Wszystkie zidentyfikowane przez Zamawiającego błędy lub podatności w Systemie lub niezgodności z określonymi wymaganiami bezpieczeństwa, Wykonawca jest zobowiązany poprawić w określonym przez Zamawiającego terminie.
8. Aktualizacja dokumentacji w trakcie realizacji zadań związanych ze świadczeniem Rozwoju Systemu obejmuje wykonanie aktualizacji dokumentacji związanych z modyfikacją Systemu. Wykonawca ma obowiązek wykonać i dostarczyć aktualną wersję dokumentacji oraz nośników wraz z każdą nową wersją Systemu i potwierdzeniem prawidłowości wykonania mechanizmu backupu dla Systemu. Aktualizacja dokumentacji jest realizowana jednocześnie przy każdej zmianie w Systemie, jeśli zmiana tego wymaga i obejmuje swoim zakresem w szczególności:
    8.1. instrukcję dla pracowników Zamawiającego;
    8.2. instrukcję dla firm audytorskich;
    8.3. instrukcję administratora Systemu;
    8.4. architekturę Systemu;
    8.5. kody źródłowe Systemu.

III. Wymagania bezpieczeństwa

Bezpieczeństwo aplikacji www musi być zgodne z wymaganiami zdefiniowanymi w standardzie OWASP (Open Web Application Security Project) Application Security Verification Standard w wersji 4.0.2 ASVS Poziom 1, rozumianych jako szereg wytycznych podczas tworzenia listy kontrolnej bezpiecznego kodowania specyficznej dla aplikacji, platformy lub organizacji:

- wszystkie komponenty aplikacji są zidentyfikowane i istnieje powód dla których zostały tam umieszczone;
- aplikacja weryfikuje cyfrową tożsamość nadawcy w trakcie komunikacji i zapewnia, że tylko upoważnione podmioty mogą się uwierzytelnić, a dane uwierzytelniające są transportowane w sposób bezpieczny;
- sesje są unikalne dla każdego użytkownika i nie mogą zostać odgadnięte lub współdzielone, są unieważniane, gdy tylko przestają być niezbędne oraz przerywane, gdy nie są wykorzystywane;
- osoby uzyskujące dostęp do aplikacji posiadają ważne dane uwierzytelniające;
- użytkownicy są powiązani z dobrze zdefiniowanymi zestawami ról i uprawnień, role i uprawnienia są chronione przed ponownym wykorzystaniem lub modyfikacją;
- wszystkie dane wejściowe są walidowane, aby zapewnić, że są poprawne i dostosowane do zamierzonych celów;
- dane z zewnętrznych źródeł lub od klientów nigdy nie powinny być traktowane jako zaufane i powinny być odpowiednio traktowane;
- wszystkie moduły kryptograficzne kończące pracę niepowodzeniem robią to w sposób bezpieczny;

- w przypadku gdy wymagana jest losowość, jest wykorzystywany odpowiedni generator liczb losowych;
- dostęp do kluczy jest zarządzany w bezpieczny sposób;
- nie występuje gromadzenie lub logowanie informacji wymagających ochrony, jeżeli nie jest to niezbędnie wymagane;
- jest zapewnione, że wszystkie logowane informacje są obsługiwane w sposób bezpieczny i chronione zgodnie z klasyfikacją tych danych;
- jest zapewnione, że logi nie są przetrzymywane nieustannie, lecz mają zdefiniowaną ważność na okres tak krótki jak to możliwe;
- aplikacja zapewnia poufność: dane powinny być chronione przed nieautoryzowanym podglądem lub ujawnieniem, zarówno podczas transmisji, jak i podczas przechowywania;
- aplikacja zapewnia integralność: dane powinny być chronione przed, nieuprawnionym tworzeniem, zmianą lub kasowaniem przez osoby nieupoważnione;
- aplikacja zapewnia dostępność: dane powinny być dostępne dla autoryzowanych użytkowników, gdy tylko są potrzebne;
- gdy dane wymagające ochrony są transmitowane to zawsze wykorzystany jest TLS tylko w bezpiecznej wersji (np. TLS 1.2+);
- wykorzystane są tylko silne algorytmy i szyfry;
- konfiguracja serwera aplikacyjnego jest odpowiednio zabezpieczona;
- odpowiedzi http zawierają bezpieczny zestaw znaków w nagłówku „content type”;
- złośliwe oprogramowanie jest eliminowane w sposób bezpieczny i kontrolowany, tak aby nie wywrzeć wpływu na resztę aplikacji;
- aplikacja nie ma wbudowanych "bomb czasowych" ani innych złośliwych kodów bazujących na czasie;
- aplikacja nie próbuje się kontaktować ze złośliwymi lub nieautoryzowanymi lokalizacjami;
- aplikacja nie ma tylnych furtek, jajek z niespodzianką (easter egg), ataków typu salami, czy błędów logicznych, które mogłyby być kontrolowane przez atakującego;
- przepływ logiki biznesowej jest sekwencyjny i uporządkowany;
- logika biznesowa zawiera ograniczania pozwalające na wykrywanie i zapobieganie zautomatyzowanym atakom;
- przepływy logiki biznesowej o wysokiej wartości biorą pod uwagę nadużycia czy nieuczciwe osoby i tym samym mają wbudowane zabezpieczenia przed podszywaniem się, modyfikowaniem danych, zaprzeczaniem, wyciekiem informacji i eskalacją uprawnień;
- niezaufane dane z plików powinny być eliminowane w sposób kontrolowany i bezpieczny;
- pliki źródłowe otrzymane z niezaufanych źródeł są przechowywane poza katalogiem głównym aplikacji (webroot) i z ograniczonymi uprawnieniami;
- wykorzystanie usług sieciowych ma adekwatne uwierzytelnianie, zarządzanie sesją i autoryzację wszystkich serwisów sieciowych;

- wykorzystanie usług sieciowych ma walidację wszystkich parametrów wejściowych, które są transmitowane z mniej do bardziej zaufanych warstw;
- aplikacja wykorzystuje aktualne biblioteki i platformy;
- aplikacja wykorzystuje bezpieczną konfigurację bazową;
- aplikacja jest wystarczająco zabezpieczona, tak aby zmiany zainicjowane przez użytkowników w konfiguracji bazowej nie powodowały słabości bezpieczeństwa lub błędów w systemie.