Załącznik nr 7 do OPZ

# Wymagania niefunkcjonalne - Bezpieczeństwo

| **ID Wymagania** | **Nazwa Wymagania** | **Treść Wymagania** | **Argumentacja** |
| --- | --- | --- | --- |
| PFRON.NF.BZP.001 | Szyfrowanie danych w warstwie wiadomości | Szyfrowanie/podpisywanie danych w warstwie wiadomości, jeśli wykorzystywane, powinno się odbywać z wykorzystaniem bezpiecznych algorytmów i protokołów (np. z wykorzystaniem WS-Security). Wykorzystywanie szyfrowania w warstwie wiadomości nie zwalnia z konieczności spełnienia wymagania dot. szyfrowania warstwy transportowej. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.002 | Szyfrowanie warstwy transportowej | Komunikacja przychodząca i wychodząca musi być zawsze szyfrowania w warstwie transportowej z wykorzystaniem TLS 1.3 oraz z wykorzystaniem bezpiecznych algorytmów. Jeżeli nie ma możliwości zaimplementowania TLS w wersji 1.3. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.003 | Szyfrowanie danych w bazie danych | System musi zapewnić silne szyfrowanie danych przechowywanych w bazie danych (włącznie z polami, rekordami i kopiami zapasowymi), aby chronić poufność, integralność i dostępność informacji.  Szyfrowanie danych w bazie danych nie powinno znacząco wpływać na wydajność systemu. System powinien być zaprojektowany w taki sposób, aby minimalizować opóźnienia spowodowane szyfrowaniem i deszyfrowaniem danych. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.004 | Uwierzytelnianie i autoryzacja | Wszystkie wywołania przychodzące i wychodzące z platform muszą być zawsze uwierzytelnione z wykorzystaniem jednego z poniższych mechanizmów, adekwatnego do danego przypadku:  Two-way SSL,  OAuth2.0,  OpenID,  SAML,  Kerberos. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.005 | Wykorzystanie API Gateway | Komunikacja przychodząca od Systemów znajdujących się poza siecią wewnętrzną PFRON, poprzez sieć publiczną (Internet, niezabezpieczony tunelem VPN) powinna odbywać się z wykorzystaniem komponentu Enterprise Gateway umieszczonego w sieci DMZ. Dla takiej komunikacji wszystkie punkty: PFRON.NF.BZP.001, PFRON.NF.BZP.002, PFRON.NF.BZP.004 muszą być spełnione. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.007 | Autoryzacja operacji | System musi zapewnić autoryzację operacji użytkownika, aby użytkownicy mieli dostęp tylko do tych funkcji systemu, do których powinni mieć dostęp na podstawie swojej roli lub uprawnień. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.008 | Centralny System zbierania logów | Możliwość zrzucania logów do centralnego Systemu zbierania logów. Powiązane z wymaganiem PFRON.NF.BZP.014.  **Argumentacja:** Mitygacja ryzyka ataków cyberprzestępców. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.009 | Dostęp do aplikacji - szyfrowanie | Dostęp do aplikacji odbywa się wyłącznie z wykorzystaniem szyfrowanego protokołu komunikacyjnego. Transmisja danych przesyłanych wewnątrz i na zewnątrz firmy musi być szyfrowana. Rozwiązanie musi poprawnie działać bez niebezpiecznych protokołów komunikacyjnych, np. SSL w wersji 3 lub niższej (wymiana danych z Systemami zewnętrznymi w oparciu o bezpieczne protokoły).  **Argumentacja:** Mitygacja ryzyka ataków cyberprzestępców. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.010 | Dostęp do kodów źródłowych | Wykonawca zobowiązuje się do udostępnienia Zamawiającemu pełnego dostępu do wszystkich kodów źródłowych, które są używane w ramach realizacji projektu.  Wykonawca powinien dostarczyć Zamawiającemu pełen zestaw kodów źródłowych, włączając w to kod aplikacji, skrypty, biblioteki, pliki konfiguracyjne i inne związane z projektem.  Dostęp do kodów źródłowych powinien obejmować wszystkie komponenty systemu, zarówno te opracowane przez Wykonawcę, jak i te, które są pochodzenia zewnętrznego (np. open source).  **Argumentacja:** Mitygacja ryzyka ataków cyberprzestępców. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.011 | Indywidualne konto Użytkownika Systemowego | Każdy Użytkownik musi posiadać indywidualne, unikalne konto. Dotyczy to Użytkowników Systemowych obsługujących formularze. | Mitygacja ryzyka ataku cyberprzestępców. Możliwość zapewnienia rozliczalności działań. |
| PFRON.NF.BZP.012 | Odporność na ataki | Rozwiązanie powinno zapewniać odporność na znane ataki, mogące narazić poufność, integralność lub autentyczność danych przetwarzanych przez aplikację. Ujawniona (także przez stronę trzecią) słabość aplikacji lub podatność na atak opisany w dostępnych publicznie źródłach będzie traktowana jak awaria aplikacji o najwyższym priorytecie. | Mitygacja ryzyka ataku cyberprzestępców |
| PFRON.NF.BZP.013 | Rejestracja czyszczenia logów z poziomu aplikacji | Rejestracja czyszczenia logów z poziomu aplikacji - integracja z SIEM. Rejestracja zdarzeń w SIEM. | Możliwość zapewnienia integralności i autentyczności historii wykonywanych operacji |
| PFRON.NF.BZP.014 | Logowanie zdarzeń | System musi zapewnić kompleksowe logowanie zdarzeń wewnętrznych oraz związanych z komunikacją wychodzącą i przychodzącą z systemów zintegrowanych. Wszystkie zdarzenia powinny być rejestrowane i logowane w systemie. | Możliwość zapewnienia integralności i autentyczności historii wykonywanych operacji |
| PFRON.NF.BZP.015 | Backupowanie logów | System musi zapewnić regularne i niezawodne backupowanie logów systemowych na niezależnym serwerze w celu zapewnienia ochrony, integralności i dostępności tych danych.  Logi zdarzeń powinny zawierać szczegółowe informacje, takie jak datę, godzinę, źródło zdarzenia, docelowe systemy, rodzaj komunikacji (np. żądanie API, odpowiedź HTTP) oraz wszelkie dodatkowe parametry i metadane dotyczące zdarzenia.  W przypadku komunikacji wychodzącej, logi powinny rejestrować wysłane żądania, otrzymane odpowiedzi oraz statusy i błędy związane z komunikacją.  W przypadku komunikacji przychodzącej, logi powinny rejestrować otrzymane żądania, wysłane odpowiedzi oraz statusy i błędy związane z komunikacją. |  |
| PFRON.NF.BZP.016 | Rozliczalność działań Użytkownika | Zapewnienie rozliczalności wszystkich działań Użytkownika. Aplikacja umożliwia generowanie raportów zawierających informacje o operacjach wykonywanych przez danego Użytkownika w danym okresie czasu lub przekazuje logi do SIEM. | Możliwość zapewnienia integralności i autentyczności historii wykonywanych operacji |
| PFRON.NF.BZP.017 | Stosowanie algorytmów kryptograficznych | Stosowanie silnych algorytmów kryptograficznych z kluczem symetrycznym o długości nie mniejszej niż 256 bitów i asymetrycznym o długości co najmniej 4096 bitów. | Mitygacja ryzyka ataków cyberprzestępców. |
| PFRON.NF.BZP.018 | Stosowanie najmniejszych koniecznych uprawnień | System musi spełniać wymóg stosowania najmniejszych koniecznych uprawnień do pracy Użytkowników i aplikacji, np. aplikacja nie może wymagać, aby podczas łączenia się do bazy danych wykorzystywane było konto administratorskie. | Mitygacja ryzyka związanego z nadmiarowym dostępem do danych. |
| PFRON.NF.BZP.019 | Uprawnienia | Możliwe jest definiowanie uprawnień Użytkownika do każdej z poszczególnych funkcji aplikacji. Uprawnienia zgodnie z metodologią RBAC. | Mitygacja ryzyka związanego z nadmiarowym dostępem do danych. |
| PFRON.NF.BZP.020 | Uwierzytelnianie wszystkich działań Użytkownika | Zapewnienie uwierzytelniania wszystkich działań Użytkownika. System musi zapewnić zarządzanie poświadczeniami Użytkowników. | Możliwość zapewnienia rozliczalności i autentyczności. |
| PFRON.NF.BZP.021 | Zautomatyzowane zamykanie sesji Użytkowników nieaktywnych | Możliwość automatycznego zamykania sesji Użytkowników nieaktywnych przez konfigurowalną długość czasu. | Możliwość zapewnienia poufności. |
| PFRON.NF.BZP.022 | Zgodność aplikacji z aktualizacjami | Zapewnienie zgodności aplikacji z aktualizacjami bezpieczeństwa Systemu operacyjnego, bazy danych i pozostałych komponentów Systemu. | Mitygacja ryzyka ataków cyberprzestępców. |
| PFRON.NF.BZP.023 | Zgodność z OWASP | Zgodność z aktualnie obowiązującą wersją OWASP. | Możliwość zapewnienia zgodności z przyjętymi standardami bezpieczeństwa. |
| PFRON.NF.BZP.024 | Zgodność z RODO | Zapewnienie możliwości pseudonimizacji lub szyfrowania danych osobowych przetwarzanych w Systemie. Zapewnienie możliwości zautomatyzowanego usuwania danych po upływie okresu ich przetwarzania z możliwością usuwania: - określonych danych osobowych po upływie przyporządkowanych dla nich okresów, - ręcznego, poza schematem obowiązującym przy usuwaniu automatycznym. Zapewnienie możliwości anonimizacji danych jako alternatywy do ich usunięcia. Zapewnienie możliwości umieszczania danych osobowych w "kwarantannie" celem uniemożliwienia dokonywania na nich jakichkolwiek operacji w związku z realizacją przez osobę fizyczną prawa do żądania ograniczenia przetwarzania danych na podstawie art. 18 RODO. | Spełnienie wymagań prawnych RODO w zakresie bezpieczeństwa przetwarzania danych osobowych. |
| PFRON.NF.BZP.025 | Przekazanie kodów źródłowych i komponentów rozwiązania | Wykonawca zobowiązuje się do przekazania Zamawiającemu wszelkich kodów źródłowych rozwiązania oraz wszystkich wykorzystanych komponentów np. open source. Wraz z przekazaniem komponentów Wykonawca musi przekazać licencję uprawniającą do korzystania z komponentu przez nieograniczony czas. |  |

## Treść ze stopki pisma

al. Jana Pawła II 13, 00-828 Warszawa, POLSKA, te. +48 22 50 55 500, [www.pfron.org.pl](http://www.pfron.org.pl)