Załącznik nr 2 do zapytania o wycenę szacunkową

Opis przedmiotu zamówienia

1. Zastosowane definicje.

1.1. Strony nadają terminom używanym w dalszej treści Umowy następujące znaczenie:

Termin	Definicja
Awaria	Wada inna niż Błąd i Usterka, powodująca całkowite zatrzymanie lub poważne zakłócenie pracy Systemu lub poszczególnych jego części, dla której nie ma alternatywnej metody wykonania danej operacji w Systemie, uniemożliwiająca korzystanie z funkcji Systemu przez jego Użytkowników tak jak było to możliwe przed wystąpieniem Awarii lub uniemożliwienie wywiązania się przez Zamawiającego z nałożonych na niego obowiązków/zadań wynikających z przepisów prawa lub wysokiego ryzyka powstania sytuacji, w której nie będzie możliwe wywiązanie się przez Zamawiającego z nałożonych na niego obowiązków/zadań wynikających z przepisów prawa.
Analiza Wstępna	Dostarczony w ramach realizacji Analizy i Projektu Produkt zawierający co najmniej: a) harmonogram realizacji Modyfikacji zawierający terminy realizacji wszystkich zadań z nią związanych (m.in. analiza, implementacja, testowanie, szkolenia, wdrożenia), b) wycenę (kwota i liczba Roboczogodzin) opartą o szacunki realizacji wszystkich zadań i podzadań, o których mowa powyżej, c) wykaz obszarów Systemu, których dotyczy Modyfikacja wraz z opisem wpływu zmian na poszczególne obszary i funkcje Systemu, d) opis konsekwencji dla dostępności, wydajności, ergonomii, bezpieczeństwa technicznego Systemu oraz bezpieczeństwa w zakresie gromadzenia oraz przetwarzania danych osobowych (w postaci zgodnej z RODO analizy ryzyka) jakie spowoduje realizacja Modyfikacji, e) wykaz oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Obcego koniecznego do wykorzystania w ramach

	realizacji Modyfikacji, f) opis oraz zakres zmian wprowadzonych przez zgłoszenie, g) opis szkoleń (opcjonalnie), h) schemat uprawnień po zmianach (opcjonalnie)
Błąd	Wada inna niż Awaria i Usterka, powodująca istotne zakłócenia pracy Systemu lub poszczególnych jego części, która jednak nie uniemożliwia Użytkownikom korzystania z funkcji Systemu, i nie stwarza ryzyka powstania sytuacji, w której nie będzie możliwe wywiązanie się przez Zamawiającego z nałożonych na niego obowiązków/zadań wynikających z przepisów prawa, polegająca w szczególności na ograniczeniu realizacji lub uciążliwości w realizacji co najmniej jednej z funkcji Systemu.
Czas Naprawy	Czas liczony od momentu dokonania Zgłoszenia Wady przez Zamawiającego do chwili udostępnienia Zamawiającemu Naprawy na Środowisku Produkcyjnym.
Czas Obejścia	Czas liczony od momentu dokonania Zgłoszenia Wady przez Zamawiającego do chwili dokonania Obejścia na Środowisku Produkcyjnym.
Dokumentacja Systemu	Wszelka dokumentacja opisująca System i Kody Źródłowe Systemu (w tym również zmiany oraz modyfikacje takiej dokumentacji), dotycząca aspektów technicznych, funkcjonalnych i użytkowych związanych z korzystaniem z Systemu, jego działaniem i rozwojem, w tym dokumentacja Systemu w wersji papierowej oraz elektronicznej. Dokumentacją Systemu jest istniejąca Dokumentacja Systemu, będąca w posiadaniu Zamawiającego na dzień podpisania Umowy, jak również Dokumentacja Systemu, którą Wykonawca zobowiązany jest zaktualizować, dostosować, wytworzyć i dostarczyć zgodnie z Umową.
Dzień Roboczy	Każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy w Rzeczpospolitej Polskiej zgodnie z ustawą z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (tekst

	jednolity: Dz. U. z 2025 r. poz. 296).
Elektroniczny System Oceny Okresowej Pracownika (ESOOP)	Moduł Systemu umożliwiający przeprowadzanie oceny okresowej pracownika w PFRON.
Godziny Robocze	Godziny od 6:00 do 18:00 w Dni Robocze.
Kierownik Projektu	Osoba kontaktowa lub podejmująca decyzje dotyczące realizacji Umowy w ramach kompetencji przyznanych w Umowie, wyznaczona przez Zamawiającego/Wykonawcę, odpowiedzialna za prawidłowe wykonywanie zobowiązań wynikających z Umowy oraz bieżący przepływ informacji pomiędzy Stronami.
Kody Źródłowe	Zestaw plików w formie czytelnej dla człowieka zawierających nieskompilowany kod oprogramowania napisany języku programowania, wynikającym z przyjętej technologii rozwiązania normalnie używanej dla umożliwienia wprowadzania modyfikacji, (w tym również komentarze oraz kody proceduralne, takie jak skrypty w języku opisu prac i skrypty do sterowania kompilacją i instalowaniem), jak również dokumentacja niezbędna do użycia takiego kodu.
Modyfikacja i Rozwój (rozwój Systemu SOF2)	Wszelkie usługi polegające na wprowadzaniu zmian w Systemie, realizowane przez Wykonawcę w zakresie opisanym w Umowie.
Naprawa	Trwałe usunięcie Wady poprzez usunięcie przyczyn powstania Wady skutkujące przywróceniem pełnej sprawności Systemu, w tym również zakończenie innych działań naprawczych.
Niedostępność Systemu	Awaria Systemu lub obniżenie parametrów wydajnościowych Systemu, opisanych w Umowie i załącznikach do Umowy.
Obejście	Zapewnienie funkcjonowania Systemu poprzez zminimalizowanie uciążliwości Wady i doprowadzenie Systemu do działania bez usuwania przyczyny wystąpienia Wady. Obejście nie stanowi Naprawy, jednak pozwala korzystać nieprzerwanie z wszystkich funkcjonalności Systemu.
Organizacja Czasu Pracy (OCP)	Moduł Systemu umożliwiający m.in. rejestrację czasu pracy pracownika PFRON, planowanie urlopów oraz

	składanie wniosków urlopowych.
Odbiór	Czynności mające na celu potwierdzenie dostarczenia Zamawiającemu usług i Produktów, powstałych w wyniku zobowiązań wynikających z Umowy.
Okno Serwisowe	Czas pomiędzy godziną 20:00 a 06:00 przeznaczony na wykonywanie wszelkich niezbędnych prac serwisowych, przeglądów, aktualizacji Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego, Oprogramowania Zamawiającego oraz Systemu, a także wgrywania nowych wersji Systemu na Środowisko Produkcyjne i Środowiska Testowe.
Opis Modelu Systemu EA	Opis Systemu uwzględniający w szczególności dziedzinę, architekturę oraz strukturę logiczną i fizyczną baz stworzony narzędziem Sparx Enterprise Architekt w wersji co najmniej 16.
Oprogramowanie Standardowe/Oprogramowanie Obce	Oprogramowanie dostarczone przez Wykonawcę, nie wytworzone w toku prac nad realizacją Systemu, stanowiące jego składnik, na którego użycie w procesach budowy, rozwoju, konfiguracji, instalacji lub użytkowania Systemu Zamawiający wyraził zgodę. Wykonawca powinien uzyskać zgodę Zamawiającego na użycie określonego Oprogramowania Standardowego/Obcego przed przystąpieniem do wszelkich prac, których efektem może być modyfikacja lub rekonfiguracja Systemu.
Oprogramowanie Systemowe i Narzędziowe	Oprogramowanie wykorzystywane na potrzeby Systemu, konieczne do poprawnego działania Systemu, inne niż Oprogramowanie Zamawiającego. Wykonawca powinien uzyskać zgodę Zamawiającego na użycie określonego Oprogramowania Systemowego i Narzędziowego przed przystąpieniem do wszelkich prac, których efektem może być modyfikacja lub rekonfiguracja Systemu.
Oprogramowanie Zamawiającego	Oprogramowanie aktualnie wykorzystywane na potrzeby Systemu, które zapewnia Zamawiający.
Pakiet Aktualizacji	Przygotowane do instalacji uaktualnienie Systemu, służące usunięciu nieprawidłowości, usprawnieniu pracy Systemu, wdrożeniu zmian.

Podwykonawca	Każdy podmiot inny niż: pracownik Wykonawcy, osoba fizyczna prowadząca działalność gospodarczą czy osoba fizyczna, z którą Wykonawca ma zawartą umowę cywilnoprawną (np. umowa o współpracy).
Portal Pracownika	Zintegrowany zbiór modułów Systemu o różnym przeznaczeniu, wspierający realizację procesów biznesowych w PFRON.
Portal Serwisowy	System informatyczny wykorzystywany przez Zamawiającego (JIRA) służący do ewidencji i obsługi Zgłoszeń, wniosków i Zamówień zapewniający niezbędny poziom wymiany informacji pomiędzy Zamawiającym a Wykonawcą.
Pomyłka Użytkownika (Pomyłka)	Błąd danych w Systemie powstały na skutek działania Użytkownika, który nie może być usunięty przez Użytkownika na poziome interfejsu użytkownika lub w terminie oczekiwanym przez Zamawiającego.
Produkt	Wszelkie programy komputerowe, dokumentacja i inne utwory, które powstają w toku wykonywania Umowy w wyniku prac Wykonawcy, w tym także wszelkie modyfikacje i opracowania innych utworów, a także materiały i informacje niepodlegające ochronie prawa autorskiego, stworzone lub dostarczone Zamawiającemu przez Wykonawcę w wyniku wykonania zobowiązań wynikających z Umowy.
Protokół Odbioru	Dokument przedstawiony przez Wykonawcę i zaakceptowany przez Zamawiającego, potwierdzający prawidłowość i zakres wykonania konkretnych usług i Produktów. Wzory Protokołów Odbioru Usługi Asysty Technicznej i Konserwacji, Modyfikacji i Rozwoju, stanowią Załącznik nr 3 do Umowy.
Przypadki Szczególne	To takie, w których Użytkownik pomimo spełnienia wymogów określonych dla Systemu, dotyczących zainstalowanego środowiska oraz mimo wsparcia konsultantów, nie może skorzystać z dowolnej funkcji Systemu przewidzianej jako jedna z dostępnych możliwości.
Pytania (Konsultacje)	Pytania (Konsultacje) dotyczące działania Systemu w ramach świadczenia Usługi Asysty Technicznej i

	Konserwacji.
Repozytorium Projektu	Narzędzie służące do rejestracji i rozliczania pracy osób realizujących Umowę po stronie Wykonawcy, środowisko skonfigurowane we wskazany przez Zamawiającego sposób, na wskazanej przez Zamawiającego infrastrukturze z wykorzystaniem wskazanego przez Zamawiającego środowiska systemu kontroli wersji (GIT), narzędziu typu case-tracker (JIRA, Microsoft Teams), lub systemie DMS (Sharepoint).
Roboczogodzina (RBH)	Jednostka miary pracochłonności wyrażająca normę ilościową pracy wykonanej przez jednego pracownika Wykonawcy w czasie jednej godziny.
RTO	Recovery Time Objective – czas niezbędny do przywrócenia Systemu po Awarii stanowiący sumę czasów naprawy Awarii z umowy hostingowej i Czasu Naprawy Awarii w ramach Usługi Asysty Technicznej i Konserwacji (ATiK).
RPO	Recovery Point Objective – punkt w czasie, do którego jest przywrócony System po Awarii.
SLA	Service Level Agreement - Poziom świadczenia usług i sposób jego pomiaru, określony w Załączniku nr 5 do OPZ
Sprzęt	Urządzenia, w szczególności sprzęt komputerowy i infrastruktura teleinformatyczna znajdująca się w posiadaniu Zamawiającego, na których działa System w okresie realizacji Umowy.
System	System, chyba że w treści Umowy wprost wskazano inaczej, w skład którego wchodzą: System SOF2, Portal Pracownika, Elektroniczny System Oceny Okresowej Pracownika (ESOOP), Organizacja Czasu Pracy (OCP).
System SOF2	Oprogramowanie eksploatowane przez Zamawiającego stanowiące System Obsługi Finansowej PFRON obejmujące następujące moduły funkcjonalne: a) Moduł Administracji; b) Moduł Kontrahentów; c) Moduł Finansowo-Księgowy;

	d) Moduł Kadrowo-Płacowy; e) Moduł Ewidencji Składników Majątkowych; f) Moduł Planowania; g) Moduł Obsługi Dofinansowań i Pożyczek; h) Moduł Windykacji Cywilno-Prawnych; i) Moduł Obsługi Elektronicznych Wyciągów Bankowych. j) Moduł Jednolitych Plików Kontrolnych k) Moduł Pism MS Word l) Moduł Emisji Dokumentów m) Moduł Logowania Operacji Opis Systemu zawiera Załącznik nr 2 do Umowy.
Środowisko Deweloperskie	Infrastruktura sprzętowo – programowa Wykonawcy, która zapewnia Wykonawcy wykonywanie m.in. czynności: 1. wprowadzania zmian do Kodu Źródłowego Systemu; 2. tworzenia i uzupełniania Dokumentacji Systemu oraz Kodów Źródłowych; 3. wytwarzania wykonywalnej i instalacyjnej wersji Systemu dla Środowiska Testowego i Środowiska Produkcyjnego; 4. przeprowadzania testów realizowanych przez Wykonawcę w wersji instalacyjnej Systemu przed przystąpieniem do testów akceptacyjnych w Środowisku Testowym.
Środowisko Produkcyjne	Środowisko informatyczne, na którym działa System.
Środowisko Testowe	Środowisko informatyczne Zamawiającego zapewniające pełne odwzorowanie warstwy funkcji Systemu posadowionego na Środowisku Produkcyjnym, analogiczne do Środowiska Produkcyjnego w zakresie systemów operacyjnych, systemów bazodanowych oraz oprogramowania aplikacyjnego mogące się różnić od Środowiska Produkcyjnego mocą obliczeniową (liczba procesorów i RAM) oraz sposobem wirtualizacji.
Umowa	Umowa zawarta między Zamawiającym a Wykonawcą wraz ze wszystkimi aneksami i Załącznikami do Umowy.
Upoważniony Pracownik	Pracownik Zamawiającego związany z realizacją

Zamawiającego	przedmiotowej Umowy.
Usługa Asysty Technicznej i Konserwacji (ATiK)	Wszelkie usługi związane z zapewnieniem bezawaryjnego działania Systemu, realizowane przez Wykonawcę w zakresie opisanym w Umowie.
Usterka	Wada niebędąca Awarią ani Błędem, powodująca zakłócenie pracy Systemu lub poszczególnych jego części mogąca mieć wpływ na jego funkcjonalność, natomiast nieograniczająca możliwości operacyjnych Systemu w sposób mogący mieć negatywny wpływ na jakość i terminowość realizacji zadań PFRON.
Użytkownik	Osoba korzystająca z Systemu lub jego poszczególnych części.
Wada	Jakiekolwiek zaburzenie pracy Systemu objawiające się poprzez jego działanie w sposób odmienny od spodziewanego, przez co należy rozumieć między innymi: 1. działanie odmienne od sposobu opisanego w Dokumentacji Systemu; 2. działanie odmienne od standardów lub zwyczajów wynikających z praktyki ustalonej w toku bieżącej eksploatacji i administracji Systemu; 3. działanie odmienne od sposobu ustalonego na mocy wszelkich innych dokumentów lub ustaleń Stron. Wada może dotyczyć wszelkich możliwych nieprawidłowości w działaniu wszystkich komponentów Systemu, może dotyczyć jego dostępności, wydajności i reaktywności, cech mających wpływ na bezpieczeństwo i ciągłość działania oraz wszystkich innych cech funkcjonalnych i pozafunkcjonalnych. Wady mogą mieć charakter Awarii, Błędu lub Usterki.
Załącznik	Każdy tekst, materiał graficzny lub też inny przedmiot, odnoszący się do treści głównego dokumentu, dołączony do niego w celu uzupełnienia bądź uprawomocnienia jego treści.
Zamówienie	Przekazanie Wykonawcy zapotrzebowania na wykonanie określonych Produktów lub innych prac

	w ramach Modyfikacji i Rozwoju
Zgłoszenie	Przekazanie Wykonawcy zawiadomienia o Wadzie, Pomyłce Użytkownika lub złożenie Pytań (Konsultacji) w ramach świadczenia Usługi Asysty Technicznej i Konserwacji oraz w okresie gwarancji.

2. Ogólny opis zamówienia.

2.1. Przedmiotem zamówienia jest świadczenie przez Wykonawcę na rzecz Zamawiającego:

2.1.1. Usługi Asysty Technicznej i Konserwacji systemu SOF2 (dalej jako „ATiK"),

a) w ramach zamówienia gwarantowanego przez okres 24 miesięcy;

b) w ramach Opcji przez okres 24 miesięcy

2.1.2. Usługi Modyfikacji i Rozwoju systemu SOF2 (dalej: rozwoju systemu SOF2) w ramach maksymalnego limitu 100 000 Roboczogodzin w ramach Opcji;

2.1.3. Usługa konsolidacji pomocniczych ksiąg rachunkowych Systemu SOF2 opisana w Załączniku nr 7 do Opisu Przedmiotu Zamówienia.

2.2. Gwarancja i rękojmia.

Wykonawca udzieli Zamawiającemu gwarancji na okres 6 miesięcy liczonych od dnia zakończenia Umowy. Gwarancja wygasa przed upływem terminu wskazanego w zdaniu poprzednim w przypadku złożenia przez Zamawiającego Wykonawcy oświadczenia o przejęciu ATiK-u oraz rozwoju Systemu przez podmiot trzeci i zwolni Wykonawcę ze świadczenia usług gwarancyjnych. Gwarancja będzie świadczona z takimi samymi parametrami jak Usługa Asysty Technicznej i Konserwacji. Szczegóły dotyczące gwarancji i rękojmi zawierają postanowienia Paragrafu 5 Umowy.

2.3. Prawa własności intelektualnej.

Szczegóły i zasady dotyczące przeniesienia autorskich majątkowych praw do Produktów oraz praw zależnych, a także udzielania i zapewniania licencji określają postanowienia Paragrafu 10 Umowy.

2.4. Licencje.

Wykonawca zobowiązuje się zapewnić Zamawiającemu licencje na korzystanie z Produktów, na warunkach i zasadach opisanych szczegółowo w Paragrafie 10 Umowy.

2.5. Inne zobowiązania.

Wykonawca zobowiązuje się wykonać inne zobowiązania na rzecz Zamawiającego, określone w Umowie i OPZ.

2.6. Szczegółowe zasady realizacji zobowiązań Wykonawcy.

Niniejszy OPZ stanowi zestawienie ramowych wymagań niezbędnych do zrealizowania celu zamówienia. Lista wymagań zawarta w dokumencie stanowi opis zakresu zamówienia przedstawiony w sposób umożliwiający skalkulowanie wyceny przez Wykonawcę. Szczegółowe zasady realizacji zobowiązań Wykonawcy w ramach Przedmiotu Zamówienia, w tym zasady świadczenia usług/prac oraz kary umowne będzie określać Umowa.

2.7. Zobowiązanie do stosowania regulacji wewnętrznych PFRON.

Wykonawca zobowiązany jest do stosowania regulacji wewnętrznych PFRON w zakresie utrzymania i rozwoju systemów informatycznych PFRON. Dokumenty zawierające regulacje wewnętrzne PFRON zostaną przekazane Wykonawcy po zawarciu Umowy.

Wymagania funkcjonalne.

3. Wymagania dotyczące Usługi Asysty Technicznej i Konserwacji.

3.1. Wymagania ogólne.

W terminie do 30 dni od zawarcia Umowy, Wykonawca zobowiązany jest do przygotowania się do świadczenia ATiK systemu SOF2.

1. W ramach przygotowania do świadczenia usługi ATiK systemu SOF2:

   1.1. Wykonawca zapozna się z należytą starannością z opisem Systemu w celu rozpoczęcia świadczenia usługi ATiK;

   1.2. Wykonawca stworzy, na swój koszt, Środowisko Deweloperskie Systemu w ramach wewnętrznej infrastruktury Wykonawcy, które będzie wykorzystywane m. in. do prac rozwojowych, przy czym Repozytorium Kodu Źródłowego, narzędzia służące do CI/CD oraz mechanizmy kompilacji i tworzenia m. in. kontenerów będą znajdować się w infrastrukturze Zamawiającego.

   1.3. Zamawiający udostępni Wykonawcy Portal Serwisowy oraz Repozytorium Projektu wspomagające świadczenie usługi ATiK, a Wykonawca zobowiązany jest, na swój koszt, do podłączenia się do Portalu Serwisowego w terminie umożliwiającym należyte wykonywanie usługi ATiK;

   1.4. Wykonawca w terminie 30 dni od dnia zawarcia Umowy (chyba, że Strony postanowią inaczej) opracuje procedury kontrolne, o których mowa w pkt ATK-114. Zamawiający zastrzega sobie prawo do zmiany procedur kontrolnych w trakcie obowiązywania Umowy, na co Wykonawca wyraża zgodę. Źródłem do opracowania procedur kontrolnych musi być dokumentacja techniczna, w tym dokumentacja administratora technicznego (przykłady procedur kontrolnych zostały wymienione w tabeli pkt ATK-114). Każda procedura kontrolna powinna zawierać co najmniej następujące informacje: autor, harmonogram, kroki procedury, sposób wykonywania procedury, wykorzystane oprogramowanie lub kod źródłowy w

przypadku oprogramowania dedykowanego Wykonawcy, rekomendowane działania naprawcze, gdy wynik procedury jest niezgodny z oczekiwanym. Procedura kontrolna może podlegać audytowi wewnętrznemu lub zewnętrznemu.

2. W Okresie Przygotowawczym, 30 dni od zawarcia Umowy, Wykonawca zobowiązany jest do wykonania Przedmiotu Umowy w pełnym zakresie, z tym, że Zamawiający nie naliczy Wykonawcy kar umownych z tytułu nie dotrzymania SLA.
3. Wykonawca, w Okresie Przygotowawczym, zobowiązany jest do przeprowadzenia audytu kompletności Dokumentacji, Kodu Źródłowego oraz konfiguracji systemu SOF2. W sytuacji wykrycia niezgodności, Wykonawca zobowiązany jest zgłosić taką informację Kierownikowi Projektu po stronie Zamawiającego. Niezależnie od wniosków z audytu Wykonawca nie może odmówić realizacji Przedmiotu Umowy w pełnym zakresie. W przypadku stwierdzenia niekompletności/nieaktualności Dokumentacji Wykonawca w ciągu 30 dni będzie zobowiązany do jej uzupełnienia.
4. Wykonawca, w Okresie Przygotowawczym zweryfikuje konfigurację narzędzia służącego do monitorowania systemu SOF2. Wykonawca ma obowiązek wprowadzić niezbędne zmiany w konfiguracji narzędzia monitorującego, tak, aby konfiguracja umożliwiała realizację Przedmiotu Umowy przez Wykonawcę w pełnym zakresie. Narzędzie monitorujące jest częścią środowiska Systemu SOF2 i podlega usłudze Asysty Technicznej i Konserwacji na tych samych zasadach co pozostałe komponenty Systemu.
5. Wykonawca w Okresie Przygotowawczym zweryfikuje działanie mechanizmów aktualizacyjnych CI/CD projektu, przedstawi raport z ich przeglądu, zarekomenduje rozwiązania i wprowadzi te mechanizmy w przypadku ich braku. Mechanizmy CI/CD muszą być zaimplementowane w ramach infrastruktury Zamawiającego.
6. Wykonawca zobowiązany jest na bieżąco, bez zbędnej zwłoki, informować Zamawiającego o wykonaniu obowiązków, o których mowa w ust. 2 powyżej. Okres Przygotowawczy może ulec skróceniu w stosunku do terminu określonego w pkt 1, w przypadku wcześniejszego zrealizowania przez Wykonawcę obowiązków, o których mowa w pkt 2 powyżej. W takim przypadku ustalenie daty zakończenia Okresu Przygotowawczego zostanie udokumentowane pisemnie przez Kierowników Projektu.
7. Po zakończeniu Okresu Przygotowania Wykonawca ponosi pełną odpowiedzialność z tytułu wykonania ATiK Systemu SOF2. Celem usunięcia wątpliwości Strony potwierdzają, że zakończenie Okresu Przygotowawczego nie wymaga podpisania przez Strony żadnego protokołu.

[**Parametry Disaster Recovery i harmonogram kopii zapasowych]**

8. Wykonawca, w terminie do 20 Dni Roboczych od dnia przekazania Wykonawcy Dokumentacji do weryfikacji (chyba, że Strony postanowią inaczej), zobowiązany jest zweryfikować obowiązujący harmonogram, zakres, sposób tworzenia kopii zapasowych

Systemu oraz scenariusze “Disaster Recovery”, a następnie ww. terminie przygotować i przedstawić Zamawiającemu do akceptacji zaktualizowane dokumenty, w taki sposób, aby mógł świadczyć ATiK Systemu. Zaktualizowane dokumenty będą podlegać Odbiorowi. W przypadku stwierdzenia braku wyżej wymienionych dokumentów, Wykonawca opracuje je na podstawie szablonów dostarczonych przez Zamawiającego.

9. Wykonawca, na podstawie analizy przedstawionej w punkcie powyżej, zobowiązany jest określić aktualne czasy RPO i RTO oraz przedstawić Zamawiającemu, w terminie 10 Dni Roboczych od dnia zakończenia weryfikacji (chyba, że Strony postanowią inaczej) planu optymalizacji parametrów RTO i RPO. Plan musi przedstawiać prace do zrealizowania, propozycje rozwiązań do wdrożenia i uruchomienia oraz harmonogram działań. Ostateczny termin wdrożenia zaproponowanych i zaakceptowanych przez Zamawiającego zmian nie może przekroczyć 90 dni, liczonych od dnia akceptacji planu optymalizacji. Zamawiający przyjmuje, że docelowe wartości RTO i RPO zostaną określone razem z Wykonawcą i gestorem Systemu SOF2 po zawarciu Umowy. Po zaakceptowaniu planu optymalizacji parametrów RTO i RPO Wykonawca przystąpi do jego realizacji. Ostateczny rezultat wykonanych prac podlega procedurze Odbioru.
10. Wykonawca zobowiązuje się do codziennego wykonywania kopii zapasowych danych Systemu w trybie ciągłym. Za zapewnienie odpowiednich narzędzi do wykonywania bieżących kopii zapasowych danych oraz odtwarzania danych z kopii zapasowej w trybie ciągłym odpowiada Wykonawca.

ATK-01. Zapewnienia ciągłości działania Systemu przez 24 godziny, 7 dni w tygodniu, 365/366 dni w roku („24/7/365/366”) przez cały okres obowiązywania Umowy z wyłączeniem Okna Serwisowego, pod warunkiem, że w ramach Okna Serwisowego realizowane są prace serwisowe wymagające wyłączenia Systemu lub powodujące tymczasową niedostępność Systemu i poszczególnych jego funkcjonalności.

ATK-02. Utrzymania i administracji Systemu w tym Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego.

ATK-03. Utrzymania wartości parametrów związanych z Usługą Asysty Technicznej i Konserwacji na warunkach opisanych w Załączniku nr 5 do OPZ.

ATK-04. Zapewnienia utrzymania parametrów wydajnościowych Systemu na poziomie określonym w Załączniku nr 1 do OPZ, pod warunkiem, że w tym czasie nie są prowadzone prace serwisowe.

ATK-05. Zapewnienia wysokiego poziomu bezpieczeństwa Systemu i danych w nim przetwarzanych, między innymi poprzez instalowanie poprawek bezpieczeństwa dla Systemu, w tym do Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego w terminie 10 Dni Roboczych od dnia wydania ich przez producenta, oraz dostosowanie Systemu do najnowszych wersji

przeglądarek internetowych w terminie 3 Dni Roboczych od dnia wydania ich przez producenta, wprowadzanie zmian konfiguracyjnych w Systemie, mających na celu zwiększenie poziomu bezpieczeństwa, zapewnienia zgodności z wymaganiami ujętymi w rozporządzeniu KRI, dokumentach wewnętrznych Funduszu - Polityce Bezpieczeństwa Teleinformatycznego, Polityce Przetwarzania Danych Osobowych i Polityce Bezpieczeństwa Informacji oraz wytycznych wynikających z obowiązujących przepisów prawa (UKSC, NIS2). Obowiązek ten dotyczy również sytuacji, gdy aktualizacji wymaga zastosowana biblioteka programistyczna, framework lub autorski kod źródłowy. W szczególnych przypadkach, Zamawiający dopuszcza możliwość wydłużenia terminu wskazanego w zdaniu poprzednim, pod warunkiem przedstawienia przez Wykonawcę pisemnego uzasadnienia. Na zmianę terminu musi wyrazić zgodę Zamawiający. Jeżeli realizacja ww. dostosowania Systemu będzie wymagała jego czasowego wyłączenia, wówczas na ten czas zawieszany jest ATK-01. Na potwierdzenie realizacji obowiązku, o którym mowa w ATK - 05 Wykonawca przedstawi raport nie później niż ostatniego dnia każdego miesiąca.

ATK-06. Przyjmowania Zgłoszeń i Naprawy Wad Systemu wraz z wyczerpującym uzasadnieniem przyczyn powstałej Wady. Zamawiający zastrzega sobie prawo do zgłaszania zastrzeżeń do treści uzasadnienia przyczyny powstałej wady, które Wykonawca jest zobowiązany uwzględnić.

ATK-07. Usuwania Wad Systemu wszystkich kategorii zgodnie z wymaganiami opisanymi w pkt 4.3 OPZ.

ATK-08. Wydawania rekomendacji dotyczących przeprowadzania zmian, aktualizacji i modernizacji Systemu.

ATK-09. Implementacji w Systemie wszystkich zaleceń powstałych w wyniku audytów bezpieczeństwa teleinformatycznego, audytów zgodności z KRI, audytów bezpieczeństwa informacji, zgodnie z przyjętym harmonogramem. Harmonogram przygotuje Wykonawca na podstawie przekazanych wyników audytu w terminie jednego tygodnia liczonego od dnia przekazania wyników audytu. Podatności niosące za sobą wysokie ryzyko lub wysokiego priorytetu muszą być usunięte z Systemu w przeciągu 10 dni od dnia przekazania wyników z audytu, chyba że Zamawiający zdecyduje inaczej. Do chwili usunięcia wyżej wspomnianych podatności Wykonawca zobligowany jest do wprowadzenia odpowiednich środków zaradczych mitygujących ryzyko wykorzystania luki podatności przez niepowołane osoby. Wykonawca implementuje zalecenia w ramach ATiK niezależnie od tego, czy realizacja danego zalecenia wymaga wprowadzenia zmian w kodzie źródłowym Systemu czy też nie oraz czy niezbędne jest wdrożenie lub zainstalowanie nowego oprogramowania Jeżeli realizacja w/w zaleceń będzie wymagała czasowego wyłączenia Systemu, wówczas na ten czas zawieszany jest ATK-01.

ATK-10. Zapewnienia stałej opieki co najmniej jednego konsultanta od strony biznesowej oraz co najmniej jednego konsultanta od strony technicznej do wsparcia przy rozwiązywaniu bieżących problemów związanych z funkcjonowaniem Systemu w Dni Robocze, w Godzinach Roboczych.

ATK-11. Wsparcie przy konstruowaniu zapytań bezpośrednich do bazy danych i dostarczania gotowych zapytań w języku SQL w celach raportowych.

ATK-12. Bieżącej aktualizacji Dokumentacji Systemu oraz Kodu Źródłowego Systemu, przechowywanych w Repozytorium Projektu, zgodnie z wymaganiami opisanymi w Załączniku nr 3 do OPZ. Wykonawca ma obowiązek wraz z Protokołem Odbioru usługi dostarczyć zaktualizowaną Dokumentację Systemu i Kody Źródłowe oraz wskazać zmiany, jakie zostały wprowadzone w ramach Usługi Asysty Technicznej i Konserwacji w okresie, za który przedstawia Protokół Odbioru. W szczególności wszelkie decyzje architektoniczne podejmowane w ramach ATiK zostaną przez Wykonawcę uwzględnione jako rekordy (ADR) w rejestrze decyzji architektonicznych.

ATK-13. Zrealizowania raz na kwartał przeglądu i aktualizacji Kodu Źródłowego i Dokumentacji Systemu zgodnie z wymaganiami opisanymi w Załączniku nr 3 do OPZ, nie później niż do ostatniego dnia danego kwartału kalendarzowego oraz przedstawienia raportu.

ATK-14. Realizacji Zgłoszeń dotyczących naprawy Wad, które dotyczą niespełniania standardu dostępności WCAG 2.1. oraz zaleceń powstałych w wyniku audytu WCAG oraz dostosowanie Systemu do wymagań opisanych WCAG 2.1. przez cały okres trwania Umowy. Zamawiający zastrzega sobie prawo do zmiany poziomu WCAG na wyższy na każdym etapie realizacji Umowy w przypadku zmiany stanu prawnego obowiązującego w Polsce bez zmiany wynagrodzenia należnego Wykonawcy, na co Wykonawca wyraża zgodę. Jeżeli realizacja w/w zaleceń będzie wymagała czasowego wyłączenia Systemu, wówczas na ten czas zawieszany jest ATK-01.

ATK-15. Aktualizacji warstw Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego nie później niż miesiąc po udostępnieniu przez producentów danego oprogramowania nowej, stabilnej jego wersji po wcześniejszym pisemnym uzgodnieniu z Zamawiającym i w terminie na jaki wyrazi zgodę Zamawiający. Wyżej wymieniony termin może zostać w szczególnych przypadkach zmieniony przez Zamawiającego na dłuższy. W przypadku krytycznych poprawek bezpieczeństwa wymaga się ich niezwłocznej instalacji. Wymóg nie dotyczy aktualizacji, do których instalacji konieczne będzie poniesienie przez Wykonawcę dodatkowych kosztów z tytułu zakupu licencji – wówczas koszty i decyzję o instalacji ponosi Zamawiający. Na czas instalacji ww. poprawek zawieszone jest ATK-01. W sytuacji, gdy aktualizacja Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego będzie wymagała zmian w Kodzie Źródłowym Systemu, Wykonawca przeprowadzi

prace aktualizacyjne wraz z dostosowaniem Kodów Źródłowych w ramach usługi ATiK. Wykonawca przed przystąpieniem do prac przedstawi harmonogram do dwóch Dni Roboczych od dnia wystąpienia potrzeby aktualizacji.

ATK-16. Instalowania na Środowisku Produkcyjnym i Środowisku Testowym, w czasie Okna Serwisowego, o ile Strony nie uzgodnią inaczej, Pakietów Aktualizacyjnych usuwających Wady mając na uwadze, że na czas instalacji zawieszone jest ATK-01. W przypadku błędów związanych z bezpieczeństwem Systemu, termin instalacji Pakietu Aktualizacyjnego musi zostać uzgodniony niezwłocznie, w formie pisemnej. Instalacja takiego Pakietu może być wykonana poza Oknem Serwisowym.

ATK-17. Instalacji Pakietu Aktualizacji w ramach MR, z zastrzeżeniem wymagań dotyczących Oprogramowania Obcego lub Narzędziowego, realizowana będzie w terminie uzgodnionym pisemnie z Zamawiającym, w czasie Okna Serwisowego, o ile Strony nie uzgodnią inaczej.

ATK-18. W Dni Robocze, w Godzinach Roboczych Wykonawca musi realizować usługi od ATK-01 do ATK-14. Ponadto, Wykonawca na każde żądanie Zamawiającego zobowiązany jest do realizacji usługi opisanej w ATK-15, ATK-16, ATK-17.

ATK-19. W Dni Robocze, pomiędzy Godzinami Roboczymi a Oknem Serwisowym Wykonawca musi realizować usługi od ATK-01, ATK-02, ATK-03, ATK-04, ATK-05, ATK-06, ATK-07 dot. Awarii. Ponadto, Wykonawca na każde żądanie Zamawiającego zobowiązany jest do realizacji usługi opisanej w ATK-15, ATK-16 oraz w przypadku ustaleń Stron ATK-17.

ATK-20. W Dni Robocze w Oknie Serwisowym Wykonawca musi realizować usługi ATK-01, ATK-02, ATK-03, ATK-04, ATK-05, ATK-06, ATK-07 dot. Awarii, ATK-09, ATK-15, ATK-16, ATK-17.

ATK-21. W dni świąteczne i ustawowo wolne od pracy Wykonawca musi realizować usługi ATK-01, ATK-02, ATK-03, ATK-04, ATK-05, ATK-06, ATK-07 dot. Awarii. Ponadto, w przypadku ustaleń Stron, Wykonawca zobowiązany jest do realizacji usługi opisanej w ATK-17.

ATK-22. W dni świąteczne i ustawowo wolne od pracy oraz w Oknie Serwisowym Wykonawca musi realizować usługi: ATK-01, ATK-02, ATK-03, ATK-04, ATK-05, ATK-06, ATK-07 dot. Awarii, ATK- 09, ATK-15, ATK-16, ATK-17.

ATK-23. Realizacji Zgłoszeń dotyczących usunięcia podatności i rekomendacji powstałych w ramach testów penetracyjnych oraz audytów zgodności z normą ISO 27001 i RODO. W przypadku, gdy usunięcie podatności wymaga modyfikacji Kodu Źródłowego, Wykonawca zrealizuje wszystkie niezbędne prace w ramach usługi ATiK. Jeżeli realizacja w/w zaleceń będzie wymagała czasowego wyłączenia Systemu, wówczas na ten czas zawieszany jest ATK-01

ATK-24. Realizacji Zgłoszeń dotyczących zmian konfiguracji infrastruktury, sieci przy współpracy z komórką Zamawiającego odpowiedzialną za infrastrukturę lub podmiotem trzecim wskazanym przez Zamawiającego. Zmiany infrastruktury mogą dotyczyć między innymi zmian w DNS, zmian adresacji IP, konfiguracji firewall, konfiguracji API, LB, konfiguracji certyfikatów, w tym certyfikatów uwierzytelniających usługi oraz certyfikatów SSL oraz WAF, a także całkowitej zmiany infrastruktury teleinformatycznej (migracja). Zamawiający przewiduje do 2 migracji w trakcie trwania Umowy.

ATK-25. W przypadku migracji środowisk Systemu do nowej infrastruktury, Wykonawca odpowiedzialny będzie za opracowanie planu migracji Systemu z obecnie eksploatowanej infrastruktury do nowej infrastruktury zawierający szczegółowe informacje o koniecznych do zapewnienia ciągłości działania krokach i czynnościach oraz zależnościach pomiędzy tymi krokami, czasem ich trwania, a także warunków realizacyjnych niezbędnych do ich wykonania (w tym zasoby, czynności, wsparcie pracowników Zamawiającego oraz działania przygotowawcze). Plan migracji powinien również zawierać szczegóły dotyczące wycofywania pojedynczych działań lub ich sekwencji, wynik analizy wymagań na zmiany w środowiskach i systemach zewnętrznych zintegrowanych z Systemem. Wykonawca w ramach przygotowania planu migracji opracuje ryzyka związane z migracją oraz plan ich mitygacji.

ATK-26. Wykonawca odpowiedzialny będzie za realizację planu migracji, o którym mowa powyżej przy wykorzystaniu zasobów własnych oraz niezbędnych zasobów Zamawiającego.

ATK-27. Zarządzania i aktualizowania na bieżąco wszystkimi poświadczeniami (login, hasło, certyfikat, token) umożliwiającymi dostęp do Systemu, maszyn wirtualnych, baz danych, API oraz Oprogramowania Standardowego, Oprogramowania Obcego, Oprogramowania Systemowego i Narzędziowego, oprogramowania Zamawiającego. Poświadczenia będą przechowywane w zaszyfrowanym sejfie (repozytorium poświadczeń), do którego dostęp będzie miał Wykonawca i Zamawiający. Szczegóły dotyczące repozytorium poświadczeń Strony uzgodnią po zawarciu Umowy. Zamawiający raz na kwartał będzie weryfikował zawartość repozytorium poświadczeń, z zastrzeżeniem pkt ATK - 28 poniżej. Wykonawca ma obowiązek backupować wszystkie certyfikaty wymagane do integracji z systemami i rejestrami zewnętrznymi i wewnętrznymi niezależnie od ich przechowywania w repozytorium poświadczeń.

ATK-28. W sytuacji, gdy repozytorium poświadczeń nie będzie zawierało kompletnych i aktualnych danych, Wykonawcy zostanie naliczona kara umowna. Wykonawca w takiej sytuacji zobowiązany jest uzupełnić repozytorium poświadczeń w terminie wyznaczonym przez Zamawiającego, a w przypadku zwłoki w wykonaniu tego obowiązku Wykonawcy zostanie naliczona kara umowna.

ATK-29. Wykonawca współodpowiedzialny będzie za przygotowanie konfiguracji bezpieczeństwa Systemu utworzonej na urządzeniu typu WAF. Po każdej zmianie konfiguracji bezpieczeństwa Wykonawca przetestuje System i przekaże ewentualne uwagi Zamawiającemu w celu jej usprawnienia. Zakres testów konfiguracji WAF oraz ilość zastosowanych próbek testowych umożliwi wypracowanie (nauczenie się) mechanizmom blokowania (WAF) algorytmów rozpoznawania ruchu prawidłowego i nieprawidłowego.

ATK-30. Konfiguracja, o której mowa powyżej, powinna przeciwdziałać atakom wyszczególnionym w OWASP TOP 10, a nie obsługiwanych przez System.

ATK-31. Wszystkie szczegóły konfiguracji WAF, LB oraz zabezpieczenia zawarte w Systemie związane z zaleceniami OWASP powinny zostać opisane w Dokumentacji technicznej Systemu.

ATK-32. Wykonawca zobowiązany jest do opracowania i bieżącej aktualizacji wykazu głównych adresów URL, z których korzysta System z uwzględnieniem wszystkich kluczowych funkcji, usług, ścieżek do zasobu, zapytań i kotwic, których blokada na WAF mogłaby mieć wpływ na prawidłowe korzystanie z Systemu.

1.2. Zasady obsługi Zgłoszeń.

ATK-33. Zgłoszenie dokonywane jest za pośrednictwem Portalu Serwisowego przez upoważnionych Pracowników Wykonawcy oraz Zamawiającego.

ATK-34. Wszystkie Zgłoszenia muszą być przez Strony rejestrowane i prezentowane w Portalu Serwisowym, w sposób pozwalający na archiwizację danych o czasie i treści Zgłoszeń oraz Obejścia i Naprawy Wad.

ATK-35. Jeżeli Wada została wykryta przez Wykonawcę, Wykonawca niezwłocznie poinformuje Zamawiającego o wystąpieniu Wady, zarejestruje Zgłoszenie w Portalu Serwisowym, nada Wadzie odpowiednią kategorię oraz przystąpi do działań zmierzających do usunięcia Wady, z tym zastrzeżeniem, że zatwierdzenie Zgłoszenia oraz ostateczna decyzja odnośnie kategorii Wady należy do Zamawiającego.

ATK-36. Zgłoszenie Wady musi zawierać między innymi:

1) wskazanie komponentu systemu, którego dotyczy zgłoszenie;
2) opis funkcjonalności Systemu, której dotyczy Wada;
3) opis zauważonych nieprawidłowości w działaniu Systemu, jeśli jest to możliwe, ilustrowanych zrzutami ekranów Systemu oraz krótkim scenariuszem sposobu uzyskania nieprawidłowości;
4) kategorię Wady.

ATK-37. W przypadku, gdy Zgłoszenie zostanie uznane przez Wykonawcę za niezasadne lub w przypadku uznania, iż Zamawiający w sposób nieprawidłowy określił kategorię Wady, Wykonawca zobowiązany jest do poinformowania Zamawiającego poprzez Portal Serwisowy o wyniku analizy Zgłoszenia, przy czym ostateczna decyzja, co do realizacji oraz co do kwalifikacji określonej Wady należy do Zamawiającego.

ATK-38. Przyjmuje się, że do skutecznego Zgłoszenia Wady dochodzi z chwilą zarejestrowania Wady w Portalu Serwisowym i zaadresowania jej do Wykonawcy.

ATK-39. W wyjątkowych sytuacjach, gdy Portal Serwisowy jest niedostępny, Zamawiający dopuszcza możliwość przekazania Zgłoszenia drogą telefoniczną lub mailową, na adres wskazany do komunikacji pomiędzy Stronami i tym samym zatwierdzenie Zgłoszenia do dalszego procedowania. W chwili przywrócenia dostępności Portalu Serwisowego, Wykonawca jest zobowiązany do niezwłocznego uzupełnienia Zgłoszenia w Portalu Serwisowym. W sytuacji opisanej w zdaniu pierwszym, przyjmuje się, że do skutecznego Zgłoszenia Wady dochodzi z chwilą przekazania Wykonawcy Zgłoszenia drogą telefoniczną lub mailową, na adres wskazany do komunikacji pomiędzy Stronami.

ATK-40. Po otrzymaniu Zgłoszenia Wykonawca przystąpi do Naprawy Wady.

ATK-41. Jeśli Wykonawca stwierdzi w trakcie działań naprawczych, że dla dokonania usunięcia Wady niezbędne jest podjęcie przez Zamawiającego określonych czynności lub uzyskania dodatkowych wyjaśnień od Zamawiającego, Wykonawca niezwłocznie zwróci się do Zamawiającego z żądaniem wykonania odpowiednich działań. Czas na dokonanie odpowiednich działań przez Zamawiającego nie będzie wliczany do Czasu Naprawy Wady.

ATK-42. Usunięcie Wady nie może prowadzić do naruszenia struktur i integralności danych, do utraty danych lub wpływać negatywnie na funkcjonowanie Systemu lub innych składników infrastruktury Zamawiającego. Wykonawca zobowiązuje się również do usunięcia Wad w sposób zapobiegający utracie jakichkolwiek danych. W przypadku, gdy wykonanie usługi wiąże się z ryzykiem utraty danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego przed przystąpieniem do usunięcia Wady.

ATK-43. Usunięcie Wady nie może naruszać zgodności Systemu z zaleceniami WCAG opisanymi w Załączniku nr 2 do OPZ.

ATK-44. Wykonawca po zainstalowaniem Pakietu Aktualizacji na Środowisku Testowym wykona testy wewnętrzne, w tym funkcjonalne, pozafunkcjonalne, bezpieczeństwa, wydajności i regresji jeśli dotyczy, zgodnie z Załącznikiem nr 4 do OPZ.

ATK-45. Zakończenie testów wewnętrznych przez Wykonawcę Pakietu Aktualizacyjnego usuwającego Wadę na Środowisku Testowym, z wynikiem pozytywnym, uznaje się za przedstawienie Zamawiającemu przez Wykonawcę raportu z testów wraz z gotowością do Odbioru Pakietu Aktualizacji. Zainstalowanie przez Wykonawcę

Pakietu Aktualizacji usuwającego Wadę na Środowisku Produkcyjnym może się odbyć wyłącznie za zgodą Zamawiającego. W wyjątkowych sytuacjach za zgodą Zamawiającego Wykonawca może zainstalować Pakiet Aktualizacji bezpośrednio na Środowisku Produkcyjnym.

ATK-46. Po zgłoszeniu gotowości Odbioru Pakietu Aktualizacji Zamawiający przystąpi niezwłocznie do jego weryfikacji, o ile strony nie postanowią inaczej.

ATK-47. Zamawiający ma prawo do weryfikacji należytego wykonania usługi dowolną metodą. Zamawiający ma w szczególności prawo przeprowadzić testy za pomocą samodzielnie zdefiniowanych scenariuszy testowych lub przez zaangażowanie podmiotu trzeciego działającego w imieniu Zamawiającego.

ATK-48. W przypadku, gdy Pakiet Aktualizacji nie usunie zgłoszonej Wady lub spowoduje pojawienie się nowej Wady w Systemie, Zgłoszenie uznaje się za niezakończone.

ATK-49. Do Czasu Naprawy Zgłoszenia nie są wliczane okresy potwierdzania przez Zamawiającego skuteczności dostarczonych poprawek oraz czas pomiędzy odbiorem przez Zamawiającego Pakietu Aktualizacji na Środowisku Testowym, a zainstalowaniem Pakietu Aktualizacji na Środowisku Produkcyjnym.

ATK-50. Wykonawca zobowiązany jest do zainstalowania Pakietu Aktualizacji najpóźniej w najbliższym Oknie Serwisowym po dokonaniu odbioru przez Zamawiającego Pakietu Aktualizacji, chyba że Zamawiający postanowi inaczej.

ATK-51. Jeżeli Wykonawca nie dokona Naprawy/Obejścia w terminach, o których mowa w Załączniku nr 5 do OPZ, Zamawiający może:

1) zawiadamiając pisemnie Wykonawcę, usunąć Wadę we własnym zakresie lub powierzyć jej usunięcie innemu podmiotowi trzeciemu na koszt Wykonawcy, co nie spowoduje utraty przysługujących Zamawiającemu uprawnień z tytułu gwarancji - przy czym koszty poniesione przez Zamawiającego przy usunięciu Wady będą potrącone z wynagrodzenia przysługującego Wykonawcy lub z zabezpieczenia należytego wykonania przedmiotu Umowy;
2) obciążyć Wykonawcę karą umowną na zasadach opisanych w Umowie.

ATK-52. Zakończenie instalacji Pakietu Aktualizacji na Środowisku Produkcyjnym kończy obsługę Zgłoszenia.

ATK-53. Zamknięcie Zgłoszenia w Portalu Serwisowym dokonywane jest po instalacji Pakietu Aktualizacji na Środowisku Produkcyjnym przez upoważnionych Pracowników Zamawiającego wskazanych w Umowie.

ATK-54. Wykonawca zobowiązany jest do uzupełnienia Zgłoszenia w Portalu Serwisowym o informacje na temat przyczyn wystąpienia Wady oraz szczegółowego opisu sposobu jej usunięcia z Systemu. Wykonawca zobowiązany jest również do zmieszczenia w danym Zgłoszeniu informacji na temat wersji Pakietu Aktualizacji wraz z datą jego

produkcyjnej implementacji. Zamawiający dopiero po uzyskaniu powyższych informacji przystąpi do zamknięcia Zgłoszenia.

ATK-55. W przypadku nieuzupełnienia Zgłoszenia o wymagane w punkcie ATK-36 oraz ATK - 54 informacje Zamawiający nie podpisze Protokołu Odbioru Usługi Asysty Technicznej i Konserwacji za dany okres rozliczeniowy.

ATK-56. W terminie 10 Dni Roboczych od zakończenia obsługi każdego zgłoszenia dotyczącego Wady, aktualizacji Systemu czy konsultacji - Wykonawca dostarczy Zamawiającemu w formie elektronicznej zaktualizowaną wersję Kodu Źródłowego Systemu oraz wersję Dokumentacji Systemu aktualizującą jej części lub całość zgodnie z zasadami opisanymi w Załączniku nr 3 OPZ. Zmiany wprowadzane przez Wykonawcę do Dokumentacji Systemu będą oznaczone wyraźnie oraz w sposób umożliwiający Zamawiającemu ich zidentyfikowanie oraz wyszukanie w tekście, w szczególności poprzez zastosowanie trybu śledzenia zmian. Wykonawca będzie aktualizował Dokumentację Systemu oraz Kod Źródłowy w ramach wynagrodzenia, o którym mowa w Umowie. Aktualizacji będzie dokonywać w sposób umożliwiający weryfikację przez Zamawiającego wprowadzonych zmian, na zasadach opisanych w Załączniku nr 3 do OPZ.

ATK-57. W przypadku stwierdzenia niespójności pomiędzy Dokumentacją Systemu a działaniem Systemu Wykonawca zobowiązany jest do usunięcia niespójności w terminie 4 Dni Roboczych od pozyskania informacji, o ile strony nie postanowią inaczej.

ATK-58. Wykonawca zobowiązany jest do uzupełnienia Zgłoszenia w Portalu Serwisowym o informacje na temat przyczyn wystąpienia Wady oraz szczegółowego opisu sposobu jej usunięcia z Systemu. Zamawiający dopiero po uzyskaniu powyższych informacji przystąpi do zamknięcia Zgłoszenia.

ATK-59. Po zamknięciu Zgłoszenia Wykonawca dostarcza zaktualizowaną Dokumentację Systemu oraz zaktualizowaną wersję Kodów Źródłowych podając w Zgłoszeniu link do zaktualizowanych dokumentów oraz do aktualizacji w Repozytorium Kodu Źródłowego.

ATK-60. W przypadku pojawienia się Wady dotykającej wszystkich Użytkowników Systemu, która zgodnie z ITIL-em określana jest mianem problemu, Wykonawca zobowiązany jest do przeprowadzenia poszerzonej, pełnej analizy przyczyn Wady po jej usunięciu oraz podjęcie w ramach usługi ATiK działań, które uniemożliwią pojawienie się tej samej Wady w przyszłości. W przypadku, gdy Wykonawca nie przeprowadzi skutecznej analizy, nie podejmie działań lub podejmie działania, które spowodują powtórne wystąpienie tego typu Wady w przyszłości, Zamawiający naliczy karę umowną, o której mowa w paragrafie 11 ust. 11 pkt 11.13 Umowy.

ATK-61. W przypadku wystąpienia takiej konieczności, Wykonawca zobowiązuje się do wsparcia i realizacji w ramach ATiK zleceń wynikających z konieczności współpracy z

organami ścigania i organami sprawiedliwości w celu udzielenia wszelkich informacji niezbędnych do przeprowadzenia postępowania.

1.3. Zasady udzielania stałych Konsultacji.

ATK-62. Konsultacje zgłaszane są w formie Pytań za pośrednictwem Portalu Serwisowego przez upoważnionych Pracowników Zamawiającego wskazanych w Umowie.

ATK-63. W wyjątkowych sytuacjach, gdy Portal Serwisowy jest niedostępny, Zamawiający dopuszcza możliwość przekazania Pytań drogą telefoniczną lub mailową, na adres wskazany do komunikacji pomiędzy Stronami oraz w ten sam sposób zatwierdzenie Pytań i ich dalsze procedowanie. W chwili przywrócenia dostępności Portalu Serwisowego, Wykonawca jest zobowiązany do niezwłocznego uzupełnienia Pytań w Portalu Serwisowym.

ATK-64. Konsultacje udzielane są za pośrednictwem Portalu Serwisowego przez upoważnionych Pracowników Wykonawcy wskazanych w Umowie.

ATK-65. Wszystkie materiały z konsultacji muszą być przez Strony rejestrowane i prezentowane w Portalu Serwisowym w sposób pozwalający na archiwizację danych o czasie i treści konsultacji (zapytań i odpowiedzi).

ATK-66. Przyjmuje się, że do skutecznego zgłoszenia Konsultacji dochodzi z chwilą jego zarejestrowania i zaadresowania na Wykonawcę w Portalu Serwisowym.

ATK-67. Jeżeli Wykonawca nie będzie w stanie udzielić odpowiedzi w czasie określonym w Załączniku nr 5 do OPZ, jest zobowiązany, za pośrednictwem Portalu Serwisowego, powiadomić o tym fakcie Zamawiającego, z którym zostanie ustalony nowy termin udzielenia odpowiedzi.

ATK-68. Jeżeli udzielenie odpowiedzi będzie wymagało przez Wykonawcę kontaktu z podmiotem trzecim (Użytkownikiem zewnętrznym), w szczególności za pośrednictwem poczty elektronicznej, telefonicznie, Wykonawca niezwłocznie, za pośrednictwem Portalu Serwisowego, poinformuje o tym fakcie Zamawiającego i uzyska jego zgodę.

ATK-69. W ramach udzielonych odpowiedzi dotyczących Przypadków Szczególnych, Wykonawca opracuje i udostępni Zamawiającemu instrukcję opisującą rozwiązanie danego Przypadku Szczególnego.

1.4. Wsparcie Analityczne

ATK-70. Wykonawca zobowiązuje się do zapewnienia Zamawiającemu wsparcia analitycznego w zakresie funkcjonalnym systemu SOF2 2.0, mającego na celu zapewnienie pełnego zrozumienia działania systemu, jego logiki biznesowej oraz zależności pomiędzy poszczególnymi elementami funkcjonalnymi. Wsparcie to

realizowane będzie w szczególności w formie konsultacji merytorycznych oraz przygotowywania materiałów analitycznych na potrzeby Zamawiającego.

ATK-71. Wsparcie analityczne obejmuje w szczególności:

1. Konsultacje funkcjonalne, obejmujące:
    a. omówienie działania poszczególnych funkcji systemu SOF2 2.0;
    b. wyjaśnienie zasad realizacji procesów biznesowych obsługiwanych przez system,
    c. wsparcie w interpretacji istniejących rozwiązań funkcjonalnych oraz ich zastosowania w praktyce.
2. Wyjaśnianie logiki biznesowej systemu, w tym:
    a. opis algorytmów realizujących reguły biznesowe,
    b. wyjaśnienie sposobu podejmowania decyzji systemowych,
    c. omówienie warunków, wyjątków oraz scenariuszy alternatywnych.
3. Analizę zależności funkcjonalnych i danych, obejmującą:
    a. relacje pomiędzy poszczególnymi funkcjami systemu,
    b. zależności pomiędzy polami danych oraz ich wpływ na działanie systemu,
    c. wpływ zmian w jednym obszarze systemu na inne jego komponenty.
4. Wyjaśnienie algorytmów obliczeniowych, w szczególności:
    a. zasad wykonywania obliczeń realizowanych przez system,
    b. źródeł danych wykorzystywanych w obliczeniach,
    c. reguł walidacji i kontroli poprawności wyników.
5. Przygotowanie materiałów analitycznych, na żądanie Zamawiającego, obejmujących w szczególności:
    a. diagramy przepływu danych,
    b. mapy procesów biznesowych,
    c. diagramy stanów,
    d. diagramy aktywności,
    e. diagramy sekwencji,
    f. inne diagramy i opracowania analityczne adekwatne do zakresu analiz.
6. Standardy i metodyka opracowań, przy czym:

a. wszystkie diagramy i materiały graficzne powinny być przygotowywane zgodnie z metodykami BPMN oraz UML,
b. zakres i poziom szczegółowości opracowań powinien być adekwatny do potrzeb Zamawiającego oraz charakteru analizowanego zagadnienia.

ATK-72. Osoba kontaktowa - Wykonawca zobowiązuje się, w ramach realizacji Umowy, do wyznaczenia jednej osoby pełniącej rolę Single Point of Contact (SPOC) odpowiedzialnej za wsparcie Zamawiającego w zakresie pytań dotyczących funkcjonalności oraz sposobu działania systemu SOF2 2.0.

ATK-73. Wszelkie Pytania Zamawiającego będą przekazywane za pośrednictwem Portalu Serwisowego.

ATK-74. Wykonawca zobowiązuje się do:
1. udzielenia odpowiedzi na zgłoszone Pytanie w terminie 1 Dnia Roboczego od momentu jego otrzymania, albo
2. w przypadku braku możliwości udzielenia pełnej odpowiedzi w tym terminie, przekazania w tym czasie informacji o przewidywanym terminie udzielenia odpowiedzi wraz z uzasadnieniem.

ATK-75. Powyższe nie wyklucza kontaktów osobistych, mailowych lub telefonicznych, o ile zajdzie taka uzasadniona potrzeba. Zarówno Zamawiający jak i Wykonawca zobowiązują się do wprowadzenia do Portalu Serwisowego wszystkich rezultatów kontaktów prowadzonych poza systemem informatycznym.

ATK-76. Szkolenia i transfer wiedzy
1. Wykonawca zobowiązuje się do zorganizowania transferu wiedzy oraz szkolenia z zakresu funkcjonalności systemu SOF2 2.0 dla Zamawiającego, mającego na celu zapewnienie pełnego zrozumienia zasad działania systemu, jego funkcjonalności oraz obsługiwanych procesów biznesowych.
2. W ramach realizacji powyższego zobowiązania Wykonawca:
    a. przeprowadzi szkolenie w formie zdalnej (on-line), stacjonarnej (off-line) lub w formie szkolenia wyjazdowego, poza siedzibami Zamawiającego i Wykonawcy, przy czym forma szkolenia zostanie uzgodniona pomiędzy Stronami,
    b. przekaże Zamawiającemu dokumentację systemu SOF2 2.0, w zakresie, w jakim dokumentacja ta nie znajduje się w posiadaniu PFRON.

ATK-77. W przypadku organizacji szkolenia wyjazdowego, Wykonawca zobowiązuje się do jego organizacji, natomiast Zamawiający zobowiązuje się do zwrotu kosztów związanych z organizacją szkolenia, po uprzednim zaakceptowaniu przez Zamawiającego planowanych kosztów. Konsultacje techniczne
1. Wykonawca zobowiązuje się do zapewnienia Zamawiającemu kompleksowego wsparcia oraz konsultacji technicznych, których celem jest umożliwienie

osobom wyznaczonym przez Zamawiającego pełnego i świadomego zrozumienia technicznych aspektów działania systemu SOF2 2.0.

2. Wsparcie techniczne obejmuje w szczególności:
   2.1. Kod źródłowy systemu
      a. omówienie struktury repozytoriów oraz organizacji kodu źródłowego,
      b. wyjaśnienie architektury aplikacji oraz podziału na warstwy i komponenty,
      c. omówienie kluczowych modułów systemu oraz ich odpowiedzialności,
      d. wskazanie miejsc implementacji kluczowej logiki biznesowej,
   2.2. Komunikację pomiędzy warstwą front-end i back-end,
      a. wyjaśnienie zasad komunikacji pomiędzy warstwami systemu,
      b. omówienie kontraktów interfejsów (API) wykorzystywanych w komunikacji,
      c. opis struktury danych przesyłanych pomiędzy warstwami,
      d. omówienie mechanizmów walidacji, obsługi błędów oraz wersjonowania kontraktów.
   2.3. Aspekty integracyjne i interfejsy API
      a. omówienie architektury integracyjnej systemu SOF2 2.0,
      b. wyjaśnienie logiki budowy zapytań (request) i odpowiedzi (response) interfejsów API,
      c. opis wykorzystywanych formatów danych oraz zasad ich serializacji,
      d. omówienie obsługi wyjątków, komunikatów błędów oraz mechanizmów bezpieczeństwa w integracjach,
      e. wskazanie zależności pomiędzy interfejsami API a procesami biznesowymi systemu.
   2.4. Model danych i baza danych
      a. omówienie logicznej i fizycznej struktury bazy danych systemu,
      b. wyjaśnienie relacji pomiędzy tabelami i rekordami,
      c. opis kluczy głównych, kluczy obcych oraz innych mechanizmów zapewniających integralność danych,
      d. omówienie zasad projektowych przyjętych w modelu danych,
      e. wskazanie zależności pomiędzy strukturą bazy danych a logiką aplikacyjną.
3. Forma i sposób realizacji wsparcia
   3.1. wsparcie realizowane będzie w formie konsultacji, warsztatów technicznych lub sesji przeglądowych,
   3.2. zakres, forma oraz harmonogram wsparcia będą każdorazowo uzgadniane pomiędzy Stronami,

3.3. wsparcie może być realizowane zdalnie lub stacjonarnie, w zależności od potrzeb Zamawiającego.

ATK-78. Wsparcie migracji

1. Wykonawca zobowiązuje się do zapewnienia Zamawiającemu kompleksowego wsparcia technicznego i analitycznego w procesie migracji danych z systemu SOF2 2.0 do systemu SOF2 3.0, w celu zapewnienia poprawności, kompletności, spójności oraz bezpieczeństwa danych migrowanych pomiędzy systemami.
2. Zakres wsparcia Wykonawcy obejmuje w szczególności:
   2.1. Przygotowanie danych źródłowych
      a. wsparcie w tworzeniu kopii zapasowych (backupów) baz danych systemu SOF2 2.0,
      b. konsultacje dotyczące strategii zabezpieczenia danych na potrzeby migracji,
      c. identyfikację danych wymagających migracji oraz danych archiwalnych lub wyłączonych z zakresu migracji.
   2.2. Analizę jakości i spójności danych
      a. identyfikację duplikatów danych oraz wsparcie w procesie deduplikacji,
      b. identyfikację rekordów niekompletnych, niespójnych lub uszkodzonych,
      c. wsparcie w oczyszczaniu baz danych z błędnych lub nieprawidłowych rekordów,
      d. analizę zależności pomiędzy danymi oraz identyfikację naruszeń integralności referencyjnej.
   2.3. Mapowanie danych pomiędzy systemami
      a. wsparcie w opracowaniu mapowania struktur danych pomiędzy systemem SOF2 2.0 a systemem SOF2 3.0,
      b. identyfikację różnic w modelach danych oraz ich wpływu na proces migracji,
      c. konsultacje dotyczące transformacji danych, w tym zmian formatów, typów danych i słowników wartości,
      d. wsparcie w definiowaniu reguł migracyjnych i walidacyjnych.
   2.4. Wsparcie techniczne procesu migracji
      a. konsultacje dotyczące narzędzi i mechanizmów migracyjnych,
      b. wsparcie w przygotowaniu i uruchamianiu skryptów migracyjnych,
      c. omówienie kolejności migracji poszczególnych obiektów danych,
      d. wsparcie w rozwiązywaniu problemów technicznych pojawiających się w trakcie migracji.

1.5. Zasady aktualizacji Systemu.

ATK-79. Aktualizacja Systemu realizowana jest dla:

1. nowych wersji Systemu wytworzonych w związku ze zmianami Sprzętu i Oprogramowania Systemowego i Narzędziowego;
2. nowych wersji lub uaktualnień Systemu lub jego poszczególnych części w ramach wersji głównej Systemu lub części Systemu, utworzonych z własnej inicjatywy przez Wykonawcę z uwzględnieniem zapisów poniżej, jako kolejne wersje Systemu lub części Systemu, zawierające usprawnienia w porównaniu z poprzednimi wersjami Sytemu lub części Sytemu;
3. dostosowania Systemu do bezwzględnie obowiązujących przepisów prawa wpływających na sposób funkcjonowania oraz funkcjonalności Systemu, w tym również określających minimalne wymagania techniczne dla systemów informatycznych eksploatowanych przez Zamawiającego.

ATK-80. Jeżeli Wykonawca opracuje samodzielnie, niezależnie od zobowiązań wynikających z Zamówienia, jakiekolwiek aktualizacje polegające na uaktualnieniu Systemu, służące do usunięcia stwierdzonych nieprawidłowości pracy Systemu, dodania nowych funkcjonalności lub uwzględnienia zmian w przepisach prawa, - Wykonawca zobowiązany jest niezwłocznie do pisemnego poinformowania Zamawiającego o fakcie opracowania powyższych uaktualnień oraz ich przedstawienia. Wykonawca zobowiązany jest również pisemnie poinformować Zamawiającego o ewentualnych skutkach zainstalowania Pakietu Aktualizacji.

ATK-81. Zasady aktualizacji Systemu obejmują również aktualizację Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego.

ATK-82. Aktualizacja Systemu przez Wykonawcę obejmuje w szczególności:

1) przygotowanie i uzgodnienie z Zamawiającym planu wdrożenia wersji Systemu, aby Zamawiający z odpowiednim wyprzedzeniem mógł poinformować Użytkowników wewnętrznych i zewnętrznych o przerwie w działaniu Systemu.
2) dostarczenie aktualizacji;
3) instalację aktualizacji na Środowiskach Testowych;
4) instalację aktualizacji na Środowisku Produkcyjnym;
5) testy Systemu na Środowisku Produkcyjnym, Środowiskach Testowych;
6) wsparcie przy uruchamianiu Systemu na wyżej wymienionych środowiskach;
7) aktualizacje Dokumentacji Systemu oraz Kodów Źródłowych w formie elektronicznej;

8) podniesienie numeru wersji Systemu.

1.6. Zasady zapewnienia kontroli i ciągłości działania Systemu oraz okresowych przeglądów.

ATK-83. W ramach Przedmiotu Zamówienia Wykonawca będzie realizował prace związane z utrzymaniem, konserwacją, administracją i aktualizacją systemów operacyjnych oraz oprogramowania firm trzecich (w tym w szczególności silników baz danych, serwerów aplikacyjnych oraz bibliotek programistycznych i narzędzi), które wykorzystywane są do prawidłowego działania Systemu, podlegające Usłudze ATiK.

W szczególności będzie realizował prace związane z:

1) monitorowaniem prawidłowości działania ww. systemów oraz oprogramowania firm trzecich. W przypadku zidentyfikowania niedostatecznej ilości zasobów Wykonawca zwróci się do Zamawiającego z wnioskiem o przydzielenie dodatkowych zasobów wraz ze wskazaniem ilości oraz określeniem powodu powstania ww. zapotrzebowania. Jeśli wskazane zasoby będą dostępne, Zamawiający przydzieli zasoby w terminie nie dłuższym niż 10 Dni Roboczych od prawidłowo przedłożonego zapotrzebowania. Za prawidłowo złożone zapotrzebowanie Zamawiający rozumie przekazanie za pośrednictwem kanału komunikacyjnego wskazanego w Umowie informacji zawierających parametr podlegający zmianie oraz powód zmiany (muszą one zawierać się w zamkniętym katalogu parametrów konfiguracyjnych maszyn wirtualnych właściwym dla ww. wirtualizatora). O zakończeniu realizacji wniosku Zamawiający poinformuje Wykonawcę w sposób analogiczny do wyżej opisanego sposobu komunikacji. Po przydzieleniu przez Zamawiającego dodatkowych zasobów w celu ich skutecznego wykorzystania Wykonawca dokona czynności rekonfiguracyjnych po stronie Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego, Oprogramowania Zamawiającego oraz Systemu. W/w czynności realizowane przez Wykonawcę muszą zostać zrealizowane w terminie nie dłuższym niż 10 Dni Roboczych od momentu poinformowania Wykonawcy o dostępności dodatkowych zasobów;
2) uaktualnianiem Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego, Oprogramowania Zamawiającego oraz Systemu do wersji aktualnie wspieranej. Przez uaktualnienie do wersji aktualnie wspieranych Zamawiający rozumie czynności związane z podniesieniem wersji Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego, Oprogramowania Zamawiającego oraz Systemu oraz wykonanie testów na Środowiskach Testowych i Produkcyjnym do wersji stabilnych posiadających aktualne wsparcie producenta tzn. posiadających możliwość pobierania i aktualizowania

oprogramowania ze stron lub z repozytoriów udostępnianych przez producenta oraz wprowadzania wszystkich zalecanych przez producenta uaktualnień, w szczególności uaktualnień dotyczących zabezpieczeń;

3) instalowaniem poprawek i łat bezpieczeństwa dla Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego, Oprogramowania Zamawiającego oraz Systemu;
4) Zarządzaniem konfiguracją poszczególnych elementów Systemu oraz wersji Oprogramowania Systemowego i Narzędziowego, Oprogramowania Standardowego/Obcego, Oprogramowania Zamawiającego w celu optymalizowania działania i zapewnienia ciągłości działania;
5) administrowaniem Oprogramowaniem Systemowym i Narzędziowym oraz Oprogramowaniem Standardowym/Obcym, Oprogramowaniem Zamawiającego oraz Systemem, w tym w szczególności dostosowywanie ww. oprogramowania w zakresie zapewniania oczekiwanego poziomu optymalizacji działania wyżej wskazanego oprogramowania;
6) analizowaniem oraz przygotowanie wytycznych w zakresie możliwości rozwojowych, realizacji zmian technologicznych mających na celu optymalizację pracy Oprogramowania Systemowego i Narzędziowego oraz Oprogramowania Standardowego/Obcego, Oprogramowania Zamawiającego oraz Systemu z jednoznacznym wskazaniem możliwości migracji do wskazanych przez Zamawiającego rozwiązań, w tym w szczególności opis czynności do wykonania, przewidywaną pracochłonność oraz potencjalne występujące ryzyka;
7) administrowaniem certyfikatami służącymi do integracji Systemu z innymi systemami zewnętrznymi i wewnętrznymi. Wykonawca ma obowiązek uzupełnić i aktualizować w tym zakresie dokumentację techniczną, tzn. dokumentacja techniczna administratora musi zawierać pełen opis procedury recertyfikacji. Wykonawca tworzy, weryfikuje i aktualizuje w ramach dokumentacji wykaz wszystkich integracji i związanych z nimi konfiguracji.
8) okresowym przeglądem kopii zapasowych. Wykonawca, w cyklach 6 miesięcznych będzie przeprowadzał przegląd kopii zapasowych Systemu polegający na testowym odtworzeniu Systemu z kopii zapasowych na środowisko wskazane przez Zamawiającego. Odtworzeniu podlegać będzie zarówno serwery aplikacyjne jak i serwery bazodanowe wraz z danymi.

ATK-84. Wykonawca określi wszystkie parametry konfiguracyjne polityk archiwizacji danych Oprogramowania objętego ATiK umożliwiających odtworzenie danych i uruchomienie wszystkich komponentów Oprogramowania. Dostarczone parametry konfiguracyjne muszą uwzględniać minimalizację parametrów RPO (Recovery Point Objective) oraz RTO (Recovery Time Objective). Na podstawie uzyskanych

informacji Zamawiający przygotuje nowe lub zmodyfikuje istniejące zadania archiwizacyjne, a Wykonawca zweryfikuje i potwierdzi poprawność ich konfiguracji oraz działania. Ww. określenie parametrów nastąpi w terminie wskazanym w punkcie 4.1 dotyczącym przygotowania do świadczenia usługi.

ATK-85. Wykonawca zobowiązany jest do okresowego analizowania i weryfikowania prawidłowości działania wszystkich zadań archiwizacyjnych. Czynności te winny być prowadzone nie rzadziej niż raz na trzy miesiące lub po każdej zmianie/modyfikacji konfiguracji polityk archiwizacji danych. Na wniosek oraz w porozumieniu z Wykonawcą, Zamawiający wskaże termin przeprowadzenia w/w prac. Nie może być on jednak dłuższy niż 21 dni kalendarzowych od zgłoszenia przez Wykonawcę gotowości do dokonania w/w czynności. Każda weryfikacja musi zostać potwierdzona obustronnie zawartym protokołem odbioru bez uwag. Zamawiający w terminie 5 Dni Roboczych od otrzymania protokołu zaakceptuje go lub zgłosi uwagi. W terminie do 14 dni kalendarzowych Wykonawca zobligowany jest do usunięcia przyczyn powstania uwag wskazanych w Protokole Odbioru. Po usunięciu przyczyn powstania uwag proces odbioru zostanie powtórzony. Zamawiający dopuszcza dwukrotne powtórzenie czynności odbiorowych.

ATK-86. Wykonawca zobowiązany jest do przeprowadzania okresowych testów procedur odzyskiwania Systemu, w tym testów scenariuszy “Disaster recovery”. Czynności te winny być prowadzone nie rzadziej niż raz na sześć miesięcy lub po każdej zmianie/modyfikacji konfiguracji polityk archiwizacji danych. Na wniosek oraz w porozumieniu z Wykonawcą Zamawiający wskaże termin przeprowadzenia w/w prac. Nie może być on jednak dłuższy niż 21 dni od zgłoszenia przez Wykonawcę gotowości do dokonania w/w czynności. Każda weryfikacja musi zostać potwierdzona obustronnie zawartym protokołem odbioru bez uwag. Zamawiający w terminie do 5 Dni Roboczych od otrzymania protokołu zaakceptuje go lub zgłosi uwagi. W terminie do 14 dni kalendarzowych Wykonawca zobligowany jest do usunięcia przyczyn powstania uwag wskazanych w protokole odbioru. Po usunięciu przyczyn powstania uwag proces odbioru zostanie powtórzony. Zamawiający dopuszcza dwukrotne powtórzenie czynności odbiorowych. W przypadku uznania, że procedury odzyskiwania Systemu po awarii lub scenariusze “Disaster recovery” są niekompletne, Wykonawca zobowiązany jest do uzupełnienia wyżej wymienionych dokumentów w terminie 3 miesięcy do dnia podpisania Umowy, w ramach usługi ATiK.

ATK-87. W przypadku uznania, że procedury odzyskiwania Systemu po Awarii lub scenariusze “Disaster recovery” są niekompletne, Wykonawca w ramach ATiK zobowiązany jest do aktualizacji wyżej wymienionych dokumentów w terminie 10 Dni Roboczych od dnia zgłoszenia przez Zamawiającego uwag.

ATK-88. Kopie Systemu wykonuje Zamawiający na podstawie parametrów wskazanych przez Wykonawcę w pkt. ATK – 84.

ATK-89. W przypadku wystąpienia konieczności odzyskania danych Systemu SOF2, Wykonawca zobowiązuje się do odzyskiwania z kopii, o których mowa w punkcie ATK-88 powyżej, danych na moment wskazany przez Zamawiającego, o ile kopia została wykonana w sposób prawidłowy lub w przypadku błędnego działania oprogramowania na moment ostatniej, poprawnie sporządzonej, codziennej kopii zapasowej Systemu SOF2. Utrata danych z Systemu SOF2 w jakimkolwiek zakresie powoduje naliczenie kary umownej, o której mowa w Paragrafie 11 ust. 9 Umowy.

ATK-90. Wykonawca na każde żądanie Zamawiającego zobowiązany jest do zasilania bazy danych Środowisk Testowych Systemu danymi z bazy danych Środowiska Produkcyjnego, przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa danych osobowych i cyberbezpieczeństwa.

ATK-91. Wykonawca dokonuje okresowych przeglądów zużycia zasobów, w tym przypadku infrastruktury chmurowej, zużycia tzw. kredytów chmurowych oraz wdraża mechanizmy rozwiązania optymalizujące wykorzystanie zasobów. Propozycje optymalizacji zasobów przygotowuje Wykonawca zgodnie z obowiązującymi wzorami lub szablonami dla danej infrastruktury. Przegląd dokonywany jest nie rzadziej niż raz w każdym kwartale roku kalendarzowego nie później niż do ostatniego dnia danego kwartału. Wykonawca w ramach przeglądów, na każde życzenie Zamawiającego przedstawia estymację zużycia zasobów na kolejny kwartał oraz weryfikuje estymację z poprzedniego przeglądu porównując z faktycznym zużyciem.

ATK-92. Wykonawca jest odpowiedzialny za odpowiedni dobór zasobów sprzętowych, aby zapewnić ciągłość działania w okresach dużego nasilenia ruchu użytkowników jak i w okresach, kiedy użytkownicy nie korzystają z Systemu. Wykonawca z odpowiednim wyprzedzeniem inicjuje i rekomenduje modyfikację zasobów Systemu, w przypadku konieczności zapewnienia jego dostępności i wydajności podczas krytycznych i obciążających System okresów.

[Plan Wyjścia]

ATK-93. Bez uszczerbku dla innych postanowień Umowy, w przypadku zakończenia współpracy Stron w ramach Umowy, niezależnie od trybu takiego zakończenia (w przypadku upływu czasu trwania Umowy, w drodze odstąpienia od Umowy, wypowiedzenia Umowy lub rozwiązania Umowy za porozumieniem Stron), Wykonawca niezwłocznie, ale nie później niż w terminie wskazanym w pkt ATK – 94 poniżej, zobowiązany jest do:

a. wydania Zamawiającemu pełnej i aktualnej na dzień rozwiązania Umowy Dokumentacji, dotyczącej wszelkich prac programistycznych zrealizowanych do daty odstąpienia, w tym pełną dokumentację powykonawczą (projektową, techniczną, funkcjonalną), w formacie umożliwiającym eksport Dokumentacji do standardowych formatów plików uzgodnionych z Zamawiającym;
b. wydania Zamawiającemu wszelkich kodów dostępu, w tym haseł i loginów pozwalających na dalsze korzystanie z Systemu (w tym haseł i loginów do baz

danych), nieprzerwaną i pełną kontynuację realizacji wszystkich czynności, które objęte były Umową na dzień wygaśnięcia Umowy, w tym utrzymywanie i rozwój Produktów, Systemu przez Zamawiającego lub osobę trzecią, której Zamawiający zleci takie usługi;

c. wydania Zamawiającemu pełnego i aktualnego Kodu Źródłowego pozwalającego na dalsze korzystanie z Systemu, nieprzerwaną i pełną kontynuację realizacji wszystkich czynności, które objęte były Umową na dzień jej wygaśnięcia, w tym utrzymywanie i rozwój Systemu przez Zamawiającego lub osobę trzecią, której Zamawiający zleci takie usługi;
d. przekazania Zamawiającemu lub osobie trzeciej wskazanej przez niego wszelkich informacji koniecznych do dalszego realizowania przedmiotu Umowy przez inny podmiot, w tym wiedzy i transferu know-how specyficznego dla całego Przedmiotu Umowy. Zobowiązanie to obejmuje w szczególności obowiązek Wykonawcy do przekazania Zamawiającemu wszelkich informacji umożliwiających osobie trzeciej kontynuację prac w ramach Przedmiotu Umowy, w tym rozwój Produktów, Systemu.

ATK-94. Wykonawca będzie zobowiązany do realizowania obowiązków wskazanych powyżej w terminie:

a. 10 Dni Roboczych od daty złożenia oświadczenia o odstąpieniu lub wypowiedzeniu przez którąkolwiek ze Stron lub daty rozwiązania Umowy za porozumieniem (chyba że w takim porozumieniu Strony wskażą inaczej) – w przypadku odstąpienia od Umowy lub wypowiedzenia Umowy w trybie natychmiastowym przez którąkolwiek ze Stron lub w razie rozwiązania Umowy za porozumieniem Stron;
b. 20 Dni Roboczych przed dniem upływu okresu trwania Umowy (włączając w to okres wypowiedzenia) – w przypadku wypowiedzenia Umowy z zachowaniem wskazanego nią okresu wypowiedzenia.

ATK-95. W celu uniknięcia wątpliwości Strony potwierdzają, że obowiązki wymienione w niniejszym rozdziale OPZ dotyczą Systemu SOF2.

ATK-96. Wynagrodzenie z tytułu wykonania zobowiązań Wykonawcy przewidzianych w niniejszym rozdziale OPZ jest zawarte w ramach wynagrodzenia opisanego Umową, wypłacanego Wykonawcy zgodnie z zasadami określonymi w Umowie. Strony zgodnie potwierdzają, że z tytułu realizacji powyższych zobowiązań Wykonawca nie jest uprawniony do żądania zapłaty żadnego dodatkowego wynagrodzenia przez Zamawiającego.

[Dostęp do Systemów Informatycznych Zamawiającego]

Informacje ogólne

ATK-97. Zamawiający oświadcza, że w celu realizacji zadań wymagających bezpośredniego logowania na maszyny wirtualne poprzez protokoły SSH (Secure Shell) lub RDP (Remote Desktop Protocol), udostępnia Wykonawcy rozwiązanie PAM (Privileged Access Management - Zarządzanie Dostępem Uprzywilejowanym). Zamawiający w chwili obecnej używa narzędzia CyberArk.

ATK-98. System CyberArk służy do zarządzania, kontroli i monitorowania dostępu uprzywilejowanego do krytycznych zasobów IT, zapewniając bezpieczne przechowywanie haseł, automatyczną rotację poświadczeń oraz rejestrowanie sesji użytkowników uprzywilejowanych.

ATK-99. Dostęp do systemów Zamawiającego jest możliwy wyłącznie poprzez system PAM.

[Licencje i ich zarządzanie]

ATK-100. Zamawiający przeznacza na potrzeby realizacji przedmiotu umowy 8 licencji CyberArk.

ATK-101. W przypadku zgłoszenia przez Wykonawcę uzasadnionej potrzeby wykorzystania większej liczby licencji niż określona w pkt ATK -100, Wykonawca zobowiązany jest do:

a. złożenia pisemnego wniosku do Zamawiającego z uzasadnieniem biznesowym, by zapewnić je na własny koszt. Zakup licencji musi być dokonany na rzecz PFRON. Wykonawca musi zakupić licencje typu EXT-VENDOR-USER-SUBS, ważne do dnia 31 marca 2027 r. lub do zakończenia świadczenia usługi przez Wykonawcę, w zależności co nastąpi pierwsze,
b. przekazania Zamawiającemu dokumentacji potwierdzającej legalność nabytych licencji.

ATK-102. Zamawiający zastrzega sobie prawo do weryfikacji zasadności wniosku o dodatkowe licencje oraz odmowy akceptacji w przypadku braku uzasadnienia.

[Zarządzanie dostępami]

ATK-103. Wykonawca zobowiązany jest do przekazania listy osób wymagających dostępu do systemu PAM, zawierającej:

a. imię i nazwisko,
b. rola w Projekcie,
c. zakres wymaganych uprawnień,
d. uzasadnienie potrzeby dostępu,
e. przewidywany okres korzystania z dostępu.

ATK-104. Zamawiający zastrzega sobie prawo do weryfikacji i akceptacji każdego wniosku o dostęp.

ATK-105. Dostępy nadawane są na zasadzie minimalnych uprawnień niezbędnych do realizacji zadań (principle of least privilege).

ATK-106. Wykonawca zobowiązany jest do niezwłocznego informowania kierownika projektu o:

a. zakończeniu współpracy z osobami posiadającymi dostęp,
b. zmianie zakresu obowiązków wymagającej modyfikacji uprawnień,
c. wszelkich incydentach bezpieczeństwa związanych z wykorzystaniem systemu PAM.

[Bezpieczeństwo i monitoring]

ATK-107. Wszystkie sesje realizowane poprzez system PAM są rejestrowane i mogą być monitorowane w czasie rzeczywistym przez Zamawiającego.

ATK-108. Wykonawca akceptuje fakt, że nagrania sesji mogą być wykorzystane w celach audytowych, bezpieczeństwa oraz rozwiązywania problemów.

ATK-109. Wykonawca zobowiązuje się do:

a. nieudostępniania danych dostępowych osobom trzecim,
b. korzystania z dostępu wyłącznie w celach związanych z realizacją umowy,
c. niezwłocznego zgłaszania wszelkich nieprawidłowości w działaniu systemu.

[Zmiana systemu PAM]

ATK-110. Zamawiający zastrzega sobie prawo do zmiany systemu PAM w trakcie trwania umowy.

ATK-111. W przypadku zmiany systemu, Zamawiający zobowiązuje się do:

a. przekazania informacji z wyprzedzeniem co najmniej 30 dni kalendarzowych,
b. określenia specyfikacji wymaganych licencji dla nowego systemu,
c. zapewnienia Wykonawcy nieprzerwanego dostępu do środowisk systemowych systemu SOF2 przez cały okres trwania migracji systemu PAM, w celu zagwarantowania ciągłości świadczenia Usługi ATIK.

ATK-112. Wykonawca ponosi pełną odpowiedzialność za działania własne jak i swoich pracowników oraz podwykonawców korzystających z systemu PAM.

ATK-113. W przypadku naruszenia zasad bezpieczeństwa, w tym:

a. próby obejścia systemu PAM,
b. udostępnienia danych dostępowych osobom nieuprawnionym,
c. wykorzystania dostępu niezgodnie z przeznaczeniem,

Zamawiający ma prawo nałożyć karę umowną zgodnie z zapisami Umowy.

ATK-114. Raport z usługi ATiK

Zawartość raportu miesięcznego z Usługi Asysty Technicznej i Konserwacji (ATiK) {wzór}

Incydenty

Zestawienie zgłoszonych incydentów w Portalu Serwisowym:

ID zgłoszenia	Typ zgłoszenia / Kategoria wady	Data zgłoszenia	Data przyjęcia	Data zamknięcia	Wymagany czas naprawy	Faktyczny czas naprawy	Temat	Uwagi
<Id systemu obsługi Incydentów>	<Konsultacja lub zgłoszenie Wady>						<czego dotyczy>	<Jeśli incydent nie został zamknięty lub

								obsłużony w wymaganym czasie>

Statystyka za okres związany z raportem:

Liczba wszystkich incydentów,

Udział przeterminowanych incydentów,

Liczba incydentów bezpieczeństwa.

Analiza SLA

SLA Systemu (dla środowiska produkcyjnego narastająco ostatnie 12 miesięcy)

Łączny czas niedostępności dla każdego środowiska objętego usługą ATiK.

Lp.	Środowisko	Niedostępność (czas w godz. min. sek.)			
		Ostatni miesiąc		Bieżący rok	
		Sumarycznie	W tym niedostępność infrastruktury	Sumarycznie	W tym niedostępność infrastruktury
	Produkcyjne				

Wykonanie usługi Backup.

Lp.	Środowisko	Nazwa/ identyfikator kopii	Typ kopii	Data wykonania	Nazwisko przekazującego dane z BIT	Sprawdzona (T/N)	Uwagi
	Produkcyjne						
	Testowe						

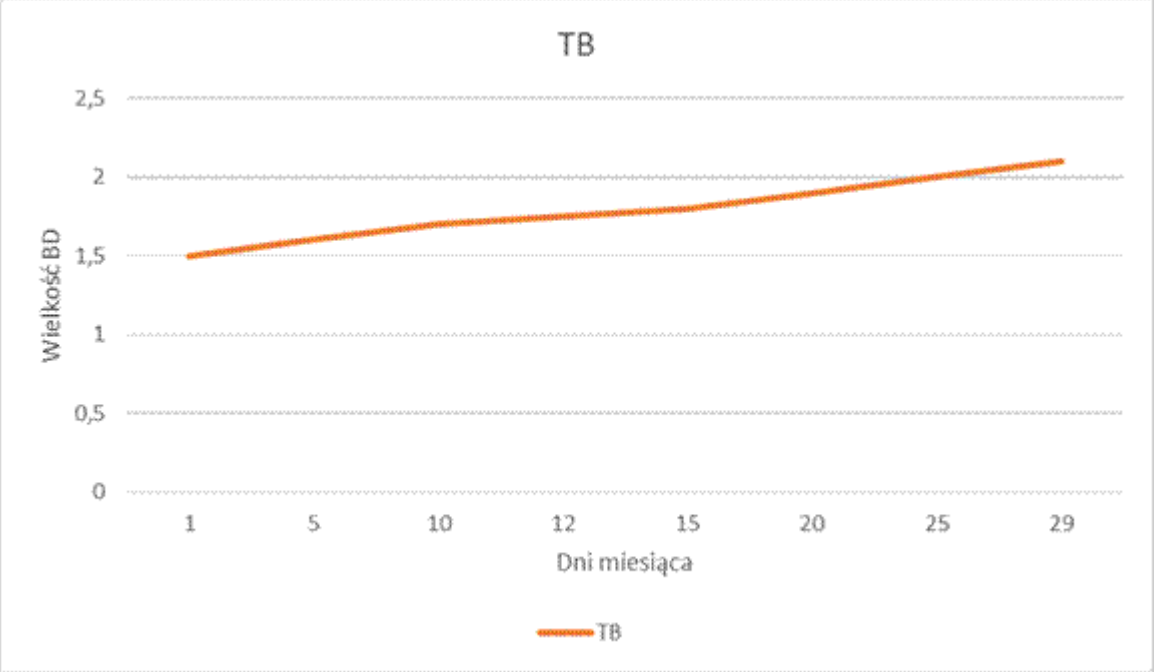
Wykonanie usługi monitorowania zasobów

Utylizacja kluczowych zasobów[].

Lp.	Środowisko	Zasoby wspólne		Nazwa VM	Dysk lokalny (% wykorzystania)
	Produkcyjne	Dyski (% wykorzystania)	Sieć zewnętrzna (% wykorzystania)		

				VM1	
				VM2	
	Testowe				

Przyrost podstawowej bazy danych systemu [TB]



Wymagane procedury kontrolne[]

Lp.	Procedura	Data wykonania	Wykryte nieprawidłowości	Podjęte działania	Uwagi
	Przykłady procedur w poniższych wierszach	<jeśli nie wykonano umieścić zapis „nie wykonano”		<Jeśli były nieprawidłowości>	Jeśli w kolumnie „Data wykonania” wpisano „nie wykonano” należy zamieścić stosowny komentarz
	Sprawdzanie czasów slow query				
	Sprawdzania ważności				

	certyfikatów				
	Weryfikacja błędów technicznych zarejestrowanych w logach na warstwie aplikacji i modyfikacja komunikacji błędów				
	Weryfikacja realizowanych przez Zamawiającego kopii bezpieczeństwa				
	Weryfikacja personelu/dostępów/uprawnień				

Wykonane przeglądy oraz aktualizacja wersji (upgrade oraz łaty) Oprogramowania Standardowego/Oprogramowania Obcego, Oprogramowania Systemowego i Narzędziowego, Oprogramowania Zamawiającego.

Lp.	Środowisko	Nazwa VM	Czynności			Uwagi
			Data przeglądu	Upgrade	Data Upgrade	
	Produkcyjne	VM1		<nazwa oprogramowania>		<nowa wersja>
				<nazwa oprogramowania>		<wycofanie wersji>
		VM2				
		….				
	Testowe					

Przegląd wersji oprogramowania (Oprogramowania Standardowego/Oprogramowania Obcego, Oprogramowania Systemowego i Narzędziowego, Oprogramowania Zamawiającego) w środowiskach Systemu

Serwer		Wersja oprogramowania (użytkowana na serwerze)	dostępna stabilna wersja oprogramowania	Uwagi/rekomendacje Wykonawcy dotyczące aktualizacji; deklarowane terminy/harmonogram aktualizacji oprogramowania
IP	hostname			

Zadania zlecone przez Zamawiającego w ramach ATiK

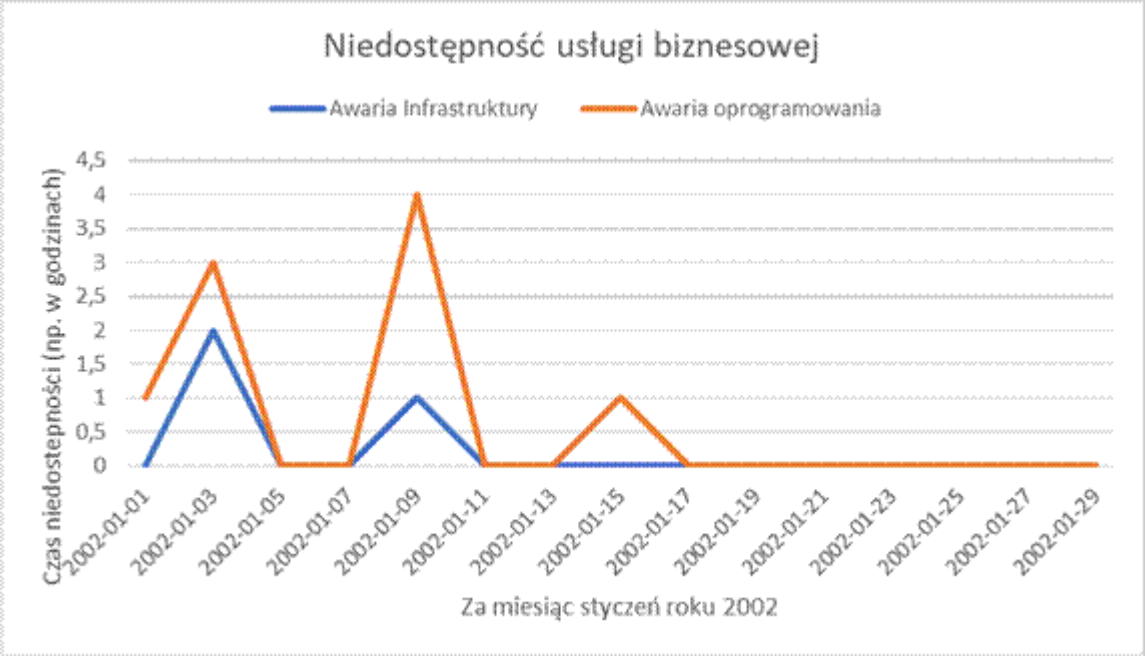
Lp.	Środowisko	Opis i przyczyna działania	Data zgłoszenia	Data zakończenia	Ocena efektów

Rekomendacje Wykonawcy

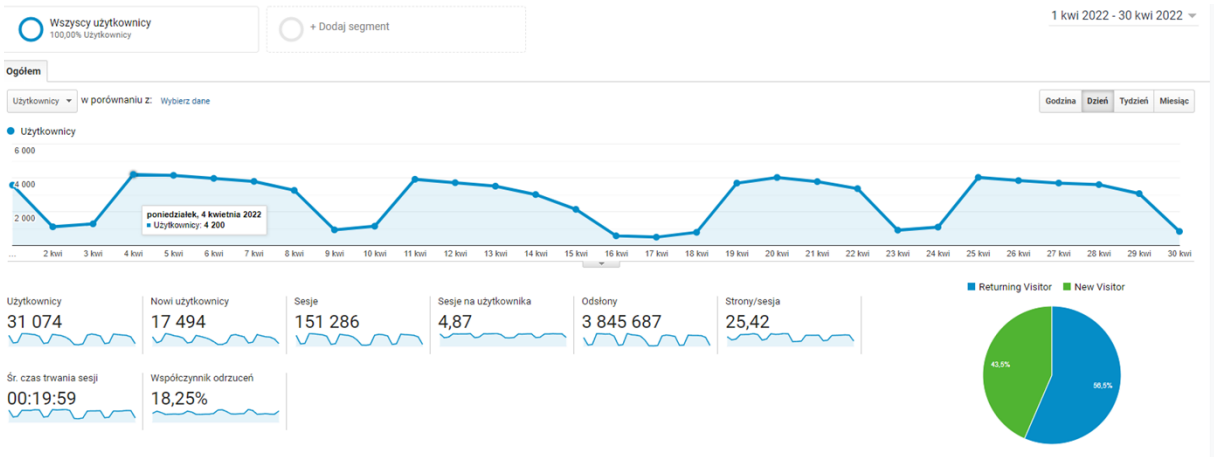
Lp.	Opis rekomendacji	Data przekazania Zamawiającemu	Decyzja Zamawiającego	Uwagi

Monitorowanie ciągłości działania Środowiska Produkcyjnego

<Przykładowy wykres niedostępności usługi poniżej>



<Przykładowe wykresy analizy korzystania z usługi przez użytkowników poniżej>



Przekazana dokumentacja:

wykaz zaktualizowanych i udostępnionych w rozliczanym okresie Dokumentów wraz z ich nr wersji, podlinkowanych w Repozytorium Projektu

Wersje i kody źródłowe:

Wykaz wgranych wersji i data ze wskazaniem w Repozytorium Kodów Źródłowych

Uwagi dodatkowe Zamawiającego:

Uwagi dodatkowe Wykonawcy:

Potwierdzam wykonanie prac

…… ……..

Data i podpis ASI Data i podpis Wykonawcy

2. Wymagania dotyczące Modyfikacji i Rozwoju.

2.1. Wymagania Ogólne.

W ramach Rozwoju Systemu Wykonawca zobowiązany jest do:

MR-01. Opracowywania i wdrażania nowych funkcjonalności Systemu oraz dokonywania wszelkich innych zmian w Systemie w zakresie wskazanym przez Zamawiającego, w tym wynikających ze zmian przepisów prawa, zaleceń audytorów, kontrolerów, zmieniających się wymogów technologicznych oraz optymalizacji procesów biznesowych i systemowych (np. parametryzację słowników, algorytmów).

MR-02. Dokonywania zmian w Systemie na potrzeby integracji z innymi systemami wykorzystywanymi przez Zamawiającego.

MR-03. Utrzymania wartości parametrów związanych z Rozwojem na warunkach opisanych w Załączniku nr 5 do OPZ.

2.2. Zasady realizacji Modyfikacji i Rozwoju.

MR-04. Wykonawca nie może odmówić realizacji złożonego Zamówienia.

MR-05. Zamawiający może wstrzymać lub zakończyć realizację każdego z etapów Modyfikacji i Rozwoju w dowolnie wybranym momencie. W razie zakończenia realizacji w trybie określonym w zdaniu poprzednim, Wykonawcy przysługuje wynagrodzenia za udokumentowane prace, z zastrzeżeniem postanowień MR-14.

MR-06. Zamawiający wymaga, aby Wykonawca przy realizacji prac w ramach Modyfikacji i Rozwoju dysponował zespołem projektowo-programowym, który może wykonać prace o zakresie nie mniejszym niż 1000 Roboczogodzin w trakcie jednego miesiąca.

MR-07. Tryb realizacji zmian może być równoległy, przy czym zakłada się, iż Wykonawca nie będzie realizował jednocześnie więcej niż 5 modyfikacji kaskadowych.

MR-08. W przypadku, gdy do realizacji prac w ramach Modyfikacji i Rozwoju niezbędne jest użycie licencji, Wykonawca zobowiązany jest do wykorzystania licencji typu open source, chyba że Zamawiający postanowi inaczej. W takim przypadku Wykonawca udzieli Zamawiającemu lub zagwarantuje udzielenie na rzecz Zamawiającego przez podmioty trzecie, przenoszalnych, bezterminowych i niewyłącznych licencji na korzystanie z takiego Oprogramowania, zgodnie z postanowieniami Umowy po udzieleniu przez Zamawiającego zgody na zastosowanie takiej licencji lub po dostarczeniu jej przez Zamawiającego. Koszt pozyskania licencji pokryje Zamawiający. Zgoda Zamawiającego wymagana jest również w przypadku konieczności zastosowania oprogramowania open-source.

MR-09. Zrealizowane prace nie mogą prowadzić do naruszenia struktur i integralności danych, do utraty danych lub wpływać negatywnie na funkcjonowanie Systemu lub innych składników infrastruktury Zamawiającego. W przypadku, gdy wykonanie

prac wiąże się z ryzykiem utraty danych, Wykonawca zobowiązany jest pisemnie poinformować o tym Zamawiającego przed przystąpieniem do realizacji prac w ramach Modyfikacji i Rozwoju.

MR-10. W przypadku, gdy realizacja prac spowoduje pojawienie się Wady w Systemie, Wykonawca zobowiązany jest do wstrzymania prac w ramach Modyfikacji i Rozwoju, do czasu skutecznego usunięcia Wady.

MR-11. Wykonawca zobowiązany jest do zapewnienia zgodności Produktów przekazywanych w ramach realizacji Modyfikacji i Rozwoju z zaleceniami WCAG zawartymi w Załączniku nr 2 do OPZ.

MR-12. Wszystkie Zamówienia oraz inne materiały z realizacji Modyfikacji i Rozwoju (w tym z testów) muszą być przez Strony rejestrowane i prezentowane w Portalu Serwisowym oraz Sharepoint.

2.3. Etapy realizacji Modyfikacji i Rozwoju Systemu

Procedura realizacji Modyfikacji i Rozwoju Systemu składa się z etapów:

- Etap 1 – analiza i projekt,
- Etap 2 – realizacja.

Etap 1 (analiza i projekt) - inicjowany jest przez Zamawiającego

MR-13. Upoważniony Pracownik Zamawiającego tworzy Zamówienie w Portalu Serwisowym zawierające: krótki opis (koncepcje) procesu biznesowego, w miarę możliwości: funkcjonalności oraz zakres danych oraz inne informacje mogące mieć wpływ na realizację Zamówienia.

MR-14. Wykonawca zobowiązany jest, by w terminie 10 dni kalendarzowych od dnia zgłoszenia Zamówienia dostarczyć nieodpłatnie wynik realizacji Analizy Wstępnej. Akceptacja Analizy Wstępnej przez Zamawiającego warunkuje dalszą realizację Modyfikacji.

MR-15. Wykonawca zgodnie z harmonogramem przedstawionym w Analizie Wstępnej, przedstawi Zamawiającemu projekt zmian w warstwach logiki biznesowej, danych, uprawnień, architektury fizycznej i logicznej Systemu, konfiguracji komponentów sprzętowych, zawierający w szczególności:

1) opis dziedziny Systemu oraz specyfikację wymagań w obszarze funkcjonalnym i (poza funkcjonalnym), które będą przedmiotem prac programistycznych (SWSI, SWB);
2) opis architektury Systemu po zmianach (głównie perspektywa biznesu, perspektywa logiczna, oraz perspektywa danych) – OAR, o ile dotyczy;
3) projekty wszystkich modułów, które będą przedmiotem prac (PMS, SKO), o ile dotyczy;

4) wycenę realizacji Etapu 2 w Roboczogodzinach z rozbiciem na poszczególne zadania składowe (podzadania) w podziale uzgodnionym z Zamawiającym;
5) zakres niezbędnego współdziałania Zamawiającego;
6) harmonogram realizacji prac;
7) informację o wpływie realizacji prac w ramach Rozwoju na integralność, wydajność oraz bezpieczeństwo Systemu;
8) wykaz niezbędnych licencji do uruchomienia zmian, o ile będą wymagane;
9) wykaz zmian w infrastrukturze informatycznej Systemu (PIS), o ile dotyczy;
10) propozycję przeprowadzenia warsztatów z nowych funkcjonalności dla Użytkowników i przedstawicieli Zamawiającego, o ile Zamówienie je obejmuje.

MR-16. Wycena, o której mowa w MR-15 musi zawierać dla każdego z punktów osobno, szacunkową liczbę Roboczogodzin niezbędną do przeprowadzenia między innymi (zakres wyceny będzie uzależniony od Zamówienia):
1) prac analitycznych,
2) prac programistycznych,
3) zmian w Kodzie Źródłowym,
4) testów,
5) warsztatów z nowych funkcjonalności dla Użytkowników i przedstawicieli Zamawiającego, jeśli Zamówienie zawiera takie zapotrzebowanie.

MR-17. Strony mogą ustalić inny termin dostarczenia Produktów Etapu 1 przez Wykonawcę.

MR-18. Strony mogą ustalić inny wykaz i zakres dla dokumentacji, o której mowa w MR -15 dostarczanej w ramach Produktów Etapu 1.

MR-19. Dopuszcza się by w ramach Zamówienia na Modyfikację i Rozwój wytwarzane były inne produkty będące częścią składową Systemu lub powiązane z Systemem, nie będące oprogramowaniem. W takim przypadku Strony mogą ustalić indywidualny tryb i zakres realizacji usługi.

MR-20. Jeśli w ramach realizacji Modyfikacji i Rozwoju istnieje techniczna możliwość zastąpienia komercyjnego rozwiązania autorstwa podmiotu trzeciego lub Wykonawcy przez oprogramowanie otwarto-źródłowe, Wykonawca jest zobowiązany uwzględnić ten fakt w przedstawionym projekcie, o którym mowa MR-15, stwarzając Zamawiającemu możliwość podjęcia decyzji w zakresie doboru konkretnego rozwiązania.

MR-21. Zamawiający zastrzega sobie prawo korzystania w trakcie wykonywania Umowy z usług osób trzecich celem kontroli wycen Zleceń w ramach Modyfikacji i Rozwoju, jakości i sposobu prowadzenia całości lub poszczególnych prac objętych Umową, dotyczących w szczególności zachowywania ustalonego Umową standardu tworzenia Produktów, w tym Kodu Źródłowego Systemu i Dokumentacji Powykonawczej, jak również do przeprowadzenia takiej kontroli samodzielnie. Osobom takim, posiadającym upoważnienie ze strony Zamawiającego, Wykonawca zobowiązany będzie udzielić niezwłocznie wszelkich informacji, danych i wyjaśnień w żądanym zakresie oraz udostępnić i zaprezentować rezultaty prowadzonych prac, jak również zapewnić możliwość ich kontroli w ramach wszystkich Środowisk. W przypadku, gdy kontrola wykaże nieprawidłowości, Wykonawca zobowiązuje się niezwłocznie wdrożyć zalecenia pokontrolne na własny koszt w terminie wskazanym przez Zamawiającego. Zamawiający zobowiązuje się, aby czynności związane z kontrolą wycen Zleceń w ramach Modyfikacji i Rozwoju, jakości i sposobu prowadzenia całości lub poszczególnych prac objętych Umową, były powierzane osobom trzecim zobowiązanym do zachowania bezstronności, poufności i ochrony interesów Wykonawcy, w tym jego know-how, metod działania i informacji handlowych. Kontrola nie będzie powierzana podmiotom, co do których istnieją uzasadnione podstawy do stwierdzenia, że prowadzą działalność bezpośrednio konkurencyjną wobec Wykonawcy w zakresie analogicznych rozwiązań objętych Przedmiotem Umowy. W przypadku kontroli wyceny pracochłonności Zlecenia przeprowadzanej na podstawie pkt MR-21, w razie powzięcia przez Zamawiającego uzasadnionych wątpliwości co do określonej przez Wykonawcę pracochłonności Zlecenia przed jego zatwierdzeniem do realizacji, stosuje się następujący tryb:

1. Zamawiający jest uprawniony do powołania niezależnego biegłego z zakresu informatyki w celu sporządzenia opinii dotyczącej pracochłonności Zlecenia;
2. Jeżeli różnica pomiędzy pracochłonnością określoną przez biegłego („RB") a pracochłonnością określoną przez Wykonawcę („RW"), liczona jako wartość bezwzględna $|RB - RW|$ i odniesiona do RW, przekracza 15% RW, wówczas podstawą ustalenia pracochłonności oraz wynagrodzenia za sporny zakres Zlecenia jest pracochłonność RB;
3. Jeżeli różnica, o której mowa w ppkt. 2 powyżej, jest równa 15% RW albo mniejsza, podstawą ustalenia pracochłonności oraz wynagrodzenia za sporny zakres Zlecenia pozostaje pracochłonność RW.
4. Koszty sporządzenia opinii biegłego ponosi:
   a) Wykonawca – w przypadku, o którym mowa w ppkt 2,
   b) Zamawiający – w przypadku, o którym mowa w ppkt 3.
5. Wykonawca niniejszym wyraża zgodę na zastosowanie mechanizmu weryfikacji określonego w niniejszym punkcie, w tym na ustalenie

pracochłonności oraz wynagrodzenia za sporny zakres Zlecenia zgodnie z opinią biegłego w przypadkach wskazanych w ppkt 2.

MR-22. Zamawiający zobowiązany jest do przekazania Wykonawcy informacji w Portalu Serwisowym czy akceptuje, czy odrzuca przedstawiony przez Wykonawcę wynik Etapu 1.

MR-23. Strony mogą dokonywać zmian i uzupełnień do materiału w trybie roboczym. Wycena wykonania Modyfikacji i Rozwoju uzgodniona na koniec Etapu 1 będzie stanowić podstawę wyliczenia wynagrodzenia za wykonanie danej usługi.

MR-24. Jeżeli Strony dokonają stosownych ustaleń przed rozpoczęciem realizacji Zamówienia, wycena Zamówienia (zadań składowych) może być aktualizowana w porozumieniu z Zamawiającym w miarę ustalania szczegółów realizacyjnych, które nie były znane lub nie zostały doprecyzowane w chwili zlecania realizacji Zamówienia. Ostateczna akceptacja wyceny czasochłonności prac należy do Zamawiającego.

MR-25. Zamawiający ma prawo zrezygnować z realizacji Etapu 2.

MR-26. Po zakończeniu Etapu 1 Zamawiający może złożyć za pośrednictwem Portalu Serwisowego Zamówienie na realizację Etapu 2.

MR-27. Poza Analizą Wstępną, produkty Etapu 1 podlegają odbiorom na zasadach opisanych w Umowie.

Etap 2 (realizacja) - inicjowany przez Zamawiającego.

MR-28. Wykonawca przystępuje do realizacji Etapu 2 po otrzymaniu od Zamawiającego Zamówienia Etapu 2.

MR-29. W wyjątkowych sytuacjach podczas trwania Etapu 2 (realizacja), ale przed przekazaniem Produktów tego Etapu do Odbioru, Zamawiający może zgłosić wniosek o zmianę wymagań, Wykonawca zobowiązany jest uwzględnić zgłoszone we wskazanym czasie zmiany wymagań. Wykonawca przedstawi Zamawiającemu poprawkę do projektu zawierającą zgłoszone zmiany wymagań, wycenę ich wykonania oraz wpływ na harmonogram realizacji w terminie 5 Dni Roboczych, o ile Strony nie postanowią inaczej.

MR-30. W uzasadnionych przypadkach Zamawiający dopuszcza zmianę terminów określonych w harmonogramie, w tym przekazania produktu do Odbioru, w stosunku do terminów uzgodnionych w ramach Etapu 1. Każdorazowa zmiana terminu w harmonogramie wymaga zgody Zamawiającego w formie dokumentowej. Zamawiający nie wyrazi zgody na zmianę terminu określonego w harmonogramie bez uzasadnienia Wykonawcy w sytuacji, gdy Wykonawca wnosi o przesunięcie terminu.

MR-31. Wykonawca przeprowadza testy wewnętrzne zgodnie z wymaganiami opisanymi w Załączniku nr 4 do OPZ na Środowisku Testowym według przygotowanych przez siebie scenariuszy testowych i potwierdza Zamawiającemu ich wykonanie poprzez wprowadzenie stosownej informacji do Portalu Serwisowego oraz zamieszczenie dokumentu Raportu z Testów (RT) w Sharepoint.

MR-32. Po przeprowadzeniu testów wewnętrznych Wykonawca zgłasza w formie dokumentowej Zamawiającemu gotowość do testów akceptacyjnych.

MR-33. Wykonawca zobowiązany jest do wgrania na Środowisko Testowe modyfikacji lub poprawek niezawierających Wad. W przypadku ich stwierdzenia, Zamawiający zastrzega sobie prawo do odstąpienia od testów akceptacyjnych, do czasu usunięcia nieprawidłowości przez Wykonawcę.

MR-34. Poinformowanie w formie dokumentowej Zamawiającego o gotowości do zainstalowania przez Wykonawcę Pakietu Aktualizacji na Środowisku Testowym uznaje się za zgłoszenie przez Wykonawcę gotowości do Odbioru realizowanego Zamówienia.

MR-35. Po zgłoszeniu gotowości do Odbioru Zamawiający przystąpi niezwłocznie do weryfikacji Pakietu Aktualizacji.

MR-36. Zamawiający ma prawo do weryfikacji należytego wykonania Zamówienia dowolną metodą. Zamawiający ma prawo przeprowadzić testy za pomocą samodzielnie zdefiniowanych scenariuszy testowych.

MR-37. Wykonawca ma obowiązek dostarczyć Zamawiającemu dokumenty, w tym raporty, scenariusze testowe wymagane w Załączniku nr 3 do OZP najpóźniej w momencie zgłoszenia Zamawiającemu przez Wykonawcę gotowości do Odbioru, o którym mowa w MR-34.

MR-38. Zamawiający w terminie określonym w harmonogramie, począwszy od daty zgłoszenia przez Wykonawcę gotowości do Odbioru, przeprowadzi testy akceptacyjne, w trakcie których zweryfikuje przedmiot Odbioru i przekaże Wykonawcy za pośrednictwem Portalu Serwisowego informację o zidentyfikowanych Wadach przedmiotu Odbioru.

MR-39. Wady będą rejestrowane w Portalu Serwisowym przez Zamawiającego oraz będą im nadawane odpowiednie kategorie:

1) Awaria,
2) Błąd,
3) Usterka (między innymi: błędy kosmetyczne, interpunkcyjne),
4) Pytanie (Konsultacje).

MR-40. W przypadku, o którym mowa w MR-39 pkt 1 Wykonawca zobowiązany jest do usunięcia Awarii w przedmiocie Odbioru w terminie 1 Dnia Roboczego od dnia jej zgłoszenia przez Zamawiającego lub w innym terminie wskazanym przez Zamawiającego.

MR-41. W przypadku, o którym mowa w MR-39 pkt 2 Wykonawca zobowiązany jest do usunięcia Błędu w przedmiocie Odbioru w terminie 2 Dni Roboczych od dnia jej zgłoszenia przez Zamawiającego lub w innym terminie wskazanym przez Zamawiającego.

MR-42. W przypadku, o którym mowa w MR-39 pkt 3 Wykonawca zobowiązany jest do usunięcia Usterki w przedmiocie Odbioru w terminie 3 Dni Roboczych od dnia jej zgłoszenia przez Zamawiającego lub w innym terminie wskazanym przez Zamawiającego.

MR-43. W przypadku, o którym mowa w MR-39 pkt 4 Wykonawca zobowiązany jest do udzielenia odpowiedzi na Pytanie (Konsultacje) w przedmiocie Odbioru w terminie 4 Dni Roboczych od dnia jej zgłoszenia przez Zamawiającego lub w innym terminie wskazanym przez Zamawiającego.

MR-44. Testy akceptacyjne po stronie Zamawiającego będą trwały do usunięcia przez Wykonawcę wszystkich zgłoszonych Wad, o ile Strony nie postanowią inaczej.

MR-45. W sytuacji, gdy w trakcie Odbioru Zamawiający zgłosi Wykonawcy co najmniej:

a. jedną Wadę, o której mowa w MR-39 pkt 1, lub

b. 11 Wad, o których mowa w MR-39 pkt 2, lub

c. 31 Wad, o których mowa w MR-39 pkt 3,

Zamawiający naliczy Wykonawcy karę umowną na zasadach i wysokościach określonych w Paragrafie 11 Umowy.

MR-46. W przypadku niektórych zmian prawnych, Zamawiający zastrzega sobie prawo do prowadzenia testów akceptacyjnych modyfikacji Systemu zleconych w ramach Etapu 2 wspólnie z Wykonawcą. W sytuacji opisanej w zdaniu poprzednim, Zamawiający odstąpi od naliczenia kar umownych, o których mowa w MR-45, za wyjątkiem sytuacji, gdy podczas testów Zamawiający zgłosi choćby jedną Wadę kategorii Awaria, wówczas Zamawiający naliczy Wykonawcy karę umowną na zasadach i w wysokości określonej w Paragrafie 11 Umowy.

MR-47. Jeżeli Wykonawca nie wykona Zamówienia w terminie określonym w harmonogramie, o którym mowa MR-15 powyżej, Zamawiający może:

1) wydłużyć termin wykonania usługi na pisemną prośbę Wykonawcy zawierającą uzasadnienie i zmiany harmonogramu,

2) obciążyć Wykonawcę karą umowną na zasadach opisanych w Umowie.

MR-48. Po zakończeniu testów akceptacyjnych, Wykonawca ma obowiązek instalacji Pakietu Aktualizacji na Środowisku Produkcyjnym w terminie uzgodnionym przez Strony.

MR-49. Nie później niż na 3 Dni Robocze przed Instalacją Pakietu Aktualizacji na Środowisku Produkcyjnym, Wykonawca dostarcza zaktualizowaną zgodnie z wymogami opisanymi w Załączniku nr 3 do OPZ, kompletną zaktualizowaną Dokumentację Systemu. Przekazana zaktualizowana Dokumentacja Systemu musi zawierać wszelkie informacje pozwalające Zamawiającemu lub podmiotom wybranym przez Zamawiającego na samodzielne korzystanie z Produktów, a także na ich samodzielne utrzymywanie i rozwój.

MR-50. Wykonawca nie później niż na 2 Dni Robocze przed Instalacją Pakietu Aktualizacji na Środowisku Produkcyjnym zobowiązany jest każdorazowo przeprowadzić warsztaty szkoleniowe z nowych funkcjonalności dla Użytkowników i przedstawicieli Zamawiającego, jeśli Zamówienie zawiera takie zapotrzebowanie.

MR-51. Instalacja Pakietu Aktualizacji na Środowisku Produkcyjnym realizowana będzie w czasie Okna Serwisowego, o ile Strony nie uzgodnią inaczej.

MR-52. Zamawiający zastrzega sobie prawo rezygnacji z instalacji Pakietu Aktualizacji na Środowisku Produkcyjnym.

MR-53. Warunkiem zakończenia realizacji Zamówienia jest:

1) Pozytywny Odbiór Zamówienia,
2) zainstalowanie przez Wykonawcę Pakietu Aktualizacji na Środowisku Produkcyjnym,
3) dostarczenie Zamawiającemu przez Wykonawcę zaktualizowanej Dokumentacji Systemu, o której mowa w MR-49,
4) przeprowadzenie przez Wykonawcę warsztatów, o których mowa w pkt MR-15 (o ile Zamówienie obejmuje warsztaty).

MR-54. Zakończenie realizacji Zamówienia potwierdzane jest poprzez jego zamknięcie w Portalu Serwisowym przez Upoważnionego Pracownika Zamawiającego wskazanego w Umowie.

MR-55. Zamknięcie Zamówienia w Portalu Serwisowym oznacza możliwość jego ujęcia w Protokole Odbioru Modyfikacji i Rozwoju, którego wzór zawiera Załącznik nr 3 do Umowy.

MR-56. Podpisanie Protokołu Odbioru, o którym mowa w MR-58 przez Zamawiającego bez zastrzeżeń jest podstawą do wystawienia przez Wykonawcę faktury.

MR-57. Z chwilą zainstalowania przez Wykonawcę Pakietu Aktualizacji na Środowisku Produkcyjnym Wykonawca obejmuje go Usługą Asysty Technicznej i Konserwacji

oraz gwarancją, o której mowa w Paragrafie 3 Umowy bez zmiany wynagrodzenia przysługującego z tytułu realizacji Umowy.

MR-58. Protokół Odbioru Zamówienia wykonanego w ramach Modyfikacji i Rozwoju zawierać będzie informację o liczbie Roboczogodzin, w ramach których Zamówienie zostało wykonane. Liczba Roboczogodzin wskazana w zaakceptowanym przez Zamawiającego Protokole Odbioru będzie podstawą do rozliczenia limitu Roboczogodzin na Rozwój określonego w niniejszej Umowie.

MR-59. Zamawiający zastrzega sobie możliwość realizacji Modyfikacji i Rozwoju w trybie alternatywnym/zwinnym, w których zakres prac, tryb i forma realizacji określane są na etapie zlecenia usługi, natomiast rozliczanie pracochłonności i określanie wynagrodzenia prac z puli Roboczogodzin przewidzianych na realizację Modyfikacji i Rozwoju ma miejsce z dołu, w oparciu o przekazywane przez Wykonawcę na bieżąco codzienne raporty i inne gromadzone na bieżąco w Repozytorium Projektu wiarygodne dowody potwierdzające fakt świadczenia usług przez poszczególnych pracowników Wykonawcy.

3. Lista załączników do Opisu Przedmiotu Zamówienia:

1) **Załącznik nr 1 do OPZ - Wymagania wydajnościowe i niezawodnościowe,**
2) **Załącznik nr 2 do OPZ - Wymagania w zakresie WCAG 2.1,**
3) **Załącznik nr 3 do OPZ -** Wymagania dla Dokumentacji,
4) **Załącznik nr 4 do OPZ -** Wymagania dotyczące testów,
5) **Załącznik nr 5 do OPZ -** Poziom świadczenia usług SLA,
6) **Załącznik nr 6 do OPZ:** Szczegółowe wymagania bezpieczeństwa w procesie utrzymania (ATiK) Systemu.
7) **Załącznik nr 7 do OPZ:** Wymagania funkcjonalne SOF2 konieczne dla przeprowadzenia konsolidacji ksiąg pomocniczych

Załącznik nr 1 do OPZ - Wymagania wydajnościowe i niezawodnościowe.

WSC-01. Wykonawca zapewni ciągłe funkcjonowanie Systemu przy założeniu, że System działa w trybie ciągłym 24 godziny na dobę, 7 dni w tygodniu, 365/366 dni w roku, a jednocześnie korzysta z niego nie więcej niż 4 tys. Użytkowników. System musi zapewnić ciągłe funkcjonowanie dla obciążeń miesięcznych na poziomie co najmniej 300 tys. przetwarzanych dokumentów pochodzących od Użytkowników.

WSC-02. Czas reakcji Systemu na zatwierdzenie formularza nie przekroczy 2 sekund. Podany czas nie dotyczy czasu wyszukiwania danych, wysyłania plików oraz generowania i dostępu do raportów oraz innych czynności związanych z wykonywaniem bardzo złożonych operacji na danych, które nie są wykonywane w trakcie codziennej, rutynowej pracy z Systemem.

WSC-03. Zamawiający jest uprawniony do prowadzenia testów sprawdzających dotrzymanie parametrów wydajnościowych Systemu. Ze strony Zamawiającego zostanie użyte narzędzie Apache JMeter (http://jmeter.apache.org).

WSC-04. Wykonawca będzie prowadził działania prewencyjne mające na celu wydłużenie czasu bezawaryjnej pracy Systemu, w tym będzie wykonywał optymalizacje Systemu oraz przeglądy nie rzadziej niż raz na kwartał, a także na żądanie Zamawiającego. Wykonawca zobowiązany jest przedstawić raport z wykonanych działań i przeglądów raz na kwartał lub na życzenie Zamawiającego

WSC-05. W przypadku konieczności wykonania prac mających na celu optymalizację działania Systemu Wykonawca bezzwłocznie poinformuje Zamawiającego o zakresie prac jaki jest z tym związany.

WSC-06. Wszelkie planowane przerwy w działaniu Systemu związane z wykonywaniem optymalizacji muszą być uzgodnione z Zamawiającym.

WSC-07. Wszystkie wymagania wyspecyfikowane w niniejszym załączniku Wykonawca będzie realizował w ramach usługi ATiK-u Systemu SOF2 oraz wynagrodzenia z tego tytułu.

Załącznik nr 2 do OPZ - Wymagania w zakresie WCAG 2.1
Spis treści

4. Wprowadzenie

System SOF2 musi być całkowicie dostępny cyfrowo dla Użytkowników z niepełnosprawnościami. Ze względu na rolę, jaką pełni PFRON, System SOF2 powinien być wzorcowy w zakresie dostępności.

Wymóg dostępności Systemu SOF2 wynika z Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.

Zgodnie z tą ustawą serwisy internetowe podmiotów realizujących zadania publiczne muszą być zgodne z WCAG 2.1 na poziomie A oraz AA.

Dodatkowo, Wykonawca jest zobowiązany do dostarczenia Systemu SOF2, który jest zgodny z WCAG 2.2 na poziomie A, AA i w wyszczególnionych przypadkach na poziomie AAA.

System musi być bezbłędny pod względem jakości kodu, zgodności z WCAG 2.2 i rzeczywistej dostępności dla wszelkich grup narażonych na wykluczenie cyfrowe.

System musi działać jednakowo z wykorzystaniem najpopularniejszych systemów:

a. Windows 11,
b. MacOS,
c. Android,
d. iOS

oraz przeglądarek internetowych:

- Google Chrome,
- Microsoft Edge,
- Mozilla Firefox,
- Safari.

5. Ogólne wymagania w zakresie dostępności cyfrowej

Przedmiotem Umowy jest zapewnienie dostępności cyfrowej Systemu zgodnie z WCAG 2.2 na poziomie A oraz AA i w wyszczególnionych poniżej przypadkach na poziomie AAA, a także zgodnie z załącznikiem do Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2023 r. poz. 1440 t.j.).

Materiałami referencyjnym odnośnie spełnienia wytycznych WCAG 2.2 są:

1. WCAG 2.2 (oficjalne wytyczne).
2. Techniques for WCAG 2.2 —dokument on-line, zawierający przydatne fragmenty kodu i przykłady zastosowania kryteriów WCAG 2.2.

W trakcie projektowania elementów interfejsów (np. menu, nawigacja, okna modalne, formularze, nawigacja okruszkowa, tabele, karuzele itp.) Wykonawca zobowiązany będzie korzystać z wzorców projektowych i dobrych praktyk, opublikowanych na stronach:

1. Wzorce projektowe ARIA opublikowane przez konsorcjum w3.org.
2. Samouczki, które dotyczą stosowania ARIA, opublikowane przez konsorcjum w3.org.

Wątpliwości dotyczące sposobów wdrażania dostępności cyfrowej będą rozstrzygane przez Zamawiającego na podstawie dokumentacji opracowanej przez www.w3.org.

6. Narzędzia testerskie wspierających budowę dostępnych cyfrowo serwisów internetowych

Niżej wymienione narzędzia wspierają tworzenie dostępnych cyfrowo serwisów oraz umożliwiają wczesne wykrycie części problemów z obszaru dostępności cyfrowej. Należy jednak pamiętać, że narzędzia automatyczne nie wykrywają wszystkich niezgodności z WCAG 2.2 – dlatego konieczna jest weryfikacja audytora WCAG oraz testy z użytkownikami z różnymi niepełnosprawnościami.

Propozycja listy narzędzi:

1. NVDA – czytnik ekranu dla systemu Windows;
2. VoiceOver – wbudowany czytnik ekranu systemu macOS/iOS/iPadOS;
3. WAVE – narzędzie do wstępnej wizualnej ewaluacji zgodności strony z WCAG 2.1 i 2.2;
4. AXE Devtools – narzędzie wspomagające badanie dostępności, generujące wstępną listę potencjalnych błędów;
5. ARC Toolkit – rozszerzenie do przeglądarki Chrome, wspierające badanie kodu strony;
6. ANDI – bookmarklet wspomagający badanie dostępności;
7. Colour Contrast Analyser – narzędzie do weryfikowania kontrastu sąsiadujących ze sobą elementów;
8. HeadingsMap – rozszerzenie pomagające określić strukturę oraz hierarchię nagłówków występujących na stronie;
9. Landmarks – rozszerzenie pomagające określić punkty orientacyjne (tak zwane landmarki) występujące na stronie;
10. Text Spacing – bookmarklet wspomagający symulację strony ze zwiększonymi odstępami w zakresie podanym w WCAG 2.1 i 2.2.

7. Wytyczne dostępności (programistyczne)

6. Zgodność składni ze specyfikacją HTML

Wszystkie strony serwisu muszą być zgodne ze standardem HTML, co można sprawdzić walidatorem, który został przygotowany przez konsorcjum w3.org.

W trakcie wdrożenia mogą wystąpić sytuacje, w których ze względu na użytą technologię możemy zaakceptować określone odstępstwa od prawidłowej składni HTML. Typowym przykładem takiej sytuacji są błędy wynikające z dodawania przez biblioteki lub frameworki (np. Angular) własnych, niestandardowych atrybutów.

Bezwzględnie natomiast wszystkie elementy kodu HTML muszą posiadać kompletne znaczniki początkowe i końcowe, być zagnieżdżane według swoich specyfikacji, nie mogą posiadać zduplikowanych atrybutów, a wszystkie użyte identyfikatory (id) muszą być unikalne.

Uwaga: Poza brakiem błędów walidacji kodu samych szablonów serwisu, także treści zapisane przy użyciu edytora wizualnego WYSIWYG nie mogą powodować problemów. Dlatego edytor wizualny powinien generować prawidłowy kod HTML.

7. **Jakość semantyczna kodu HTML**

Podstawowym warunkiem dostępności jest prawidłowe — adekwatne stosowanie znaczników HTML. Najprościej rzecz ujmując, serwis musi być realizowany w pełnej zgodności ze specyfikacją HTML5.

Przykłady poprawności semantycznej:

W ramach prac nad serwisem należy pamiętać, że poszczególne elementy należy wykonać w określony sposób:

1. Linki za pomocą znacznika <a>, czyli natywnego semantycznego znacznika HTML. Jeśli jest to niemożliwe dopuszczalne są również niesemantyczne elementy wraz z odpowiednią rolą role="link", pod warunkiem, że zadbano o możliwość ustawienia na nich fokusu klawiatury (tabindex="0") oraz przypisano w JavaScript reagowanie nie tylko na zdarzenia typu click, ale również keydown (reagujący na klawisz Enter);
2. Nagłówki za pomocą znaczników <h1>...<h6> (przy czym nagłówek <h1> powinien występować tylko raz), czyli natywnych semantycznych znaczników HTML. Jeśli jest to niemożliwe dopuszczalne są również niesemantyczne elementy wraz z odpowiednią rolą, na przykład dla nagłówka poziomu 1 role="heading" aria-level="1";
3. Przyciski za pomocą znaczników <button> lub <input type="button">, czyli natywnego semantycznego znacznika HTML. Jeśli jest to niemożliwe dopuszczalne są również niesemantyczne elementy wraz z odpowiednią rolą role="button", pod warunkiem, że zadbano o możliwość ustawienia na nich fokusu klawiatury (tabindex="0") oraz przypisano w JavaScript reagowanie nie tylko na zdarzenia typu click, ale również keydown (reagujący na klawisz Enter oraz klawisz Spacja);
4. Listy za pomocą znaczników / i <li> dla poszczególnych elementów;
5. Rozwijane listy formularzy za pomocą znaczników <select>/<option>.

Jednocześnie Zamawiający wskazuje, że **stosowanie ról ARIA jako zamiennika natywnego HTML powinno mieć charakter wyjątkowy**. W przypadku zastosowania znaczników ARIA zamiast semantycznych elementów HTML, **wszystkie stany, właściwości oraz zachowania charakterystyczne dla danego** komponentu (m.in. obsługa klawiatury, fokus, stany aktywne, nieaktywne, rozwinięte, zwinięte, reakcje na zdarzenia) **muszą zostać dodatkowo zaimplementowane po stronie aplikacji**, tak aby ich funkcjonowanie było w pełni równoważne z natywnymi komponentami HTML. Odpowiedzialność za zapewnienie tej równoważności spoczywa na Wykonawcy.

Przykłady błędów semantycznych:

Należy unikać poniższych rozwiązań.

1. Link wykonany za pomocą (oskryptowany JavaScript);
2. Nagłówek w formie **<p class="heading">;**
3. Lista rozwijana w formularzu, wykonana za pomocą znaczników listy /<li>.

8. Uzupełnienia semantyczne za pomocą ARIA

Atrybuty ARIA muszą być uzupełnieniem semantyki HTML. To technologia przeznaczona przede wszystkim dla użytkowników czytników ekranu. Szczególnie ważne jest jej stosowanie w komponentach stron internetowych, które opierają się na rozbudowanej interakcji JavaScript.

Stosowanie atrybutów ARIA można podzielić na dwie części:

1. uzupełnienie głównych bloków serwisu o punkty orientacyjne;
2. dodatki do formularzy lub takich komponentów stron, jak karuzele, zakładki (**tabs**), menu rozwijane, bloki rozwijane, okna modalne, alerty, slidery.

Głównymi źródłami informacji jak stosować ARIA powinny być dla Ciebie dokumentacje ARIA Techniques for WCAG 2.2 oraz ARIA Authoring Practices Guide (APG).

9. Tytuły stron Systemu internetowego

Wszystkie tytuły stron serwisu muszą być automatycznie generowane i zawierać informacje, które pozwolą użytkownikowi dowiedzieć się, co jest treścią danej strony.

Przykłady:

1. Strona główna serwisu powinna mieć tytuł — „Serwis informacyjny iPFRON+”.
2. Strona „Program Wsparcie Inicjatyw” powinna mieć tytuł — „Program Wsparcie Inicjatyw – Serwis informacyjny iPFRON+”.

Wszystkie strony mają mieć tytuł wg zasady - od szczegółu do ogółu.

Do uzgodnienia pozostanie kwestia, ile elementów ścieżki ma być widocznych w tytule:

1. tytuł strony + nazwa serwisu lub
2. tytuł stron + nazwa działu + np. nazwa nadrzędnego działu + nazwa serwisu.

Zgodnie z wymaganiami dla systemu zarządzania treścią (CMS), opis dodatkowych modułów i funkcjonalności CMS oraz CMS serwisu - Redaktor musi mieć możliwość indywidualnego definiowania zawartości atrybutu metatagu **title**, niezależnie od tytułu redakcyjnego.

10. Oznaczenie języka strony i treści

Język naturalny treści na stronie musi być zawsze oznaczony odpowiednim atrybutem lang. W założeniu wszystkie strony serwisu będą miały atrybut lang o treści **"pl"** lub **"pl-PL"**.
W przypadku wersji serwisu w języku innym niż polski, atrybut powinien zawierać znacznik odpowiadający naturalnemu językowi strony, przykładowo dla wersji serwisu w języku ukraińskim będzie to **lang="uk"** lub **lang="uk-UA"**.

Dodatkowo należy zapewnić redaktorom serwisu w edytorze **WYSIWYG** możliwość oznaczenia takim atrybutem dowolnego ciągu znaków, tak by użytkownik korzystający z technologii asystujących mógł zorientować się, że treść jest w innym języku, niż domyślny język strony.

11. Nagłówki stałe

Występujące w serwisie stałe bloki treści i bloki funkcjonalne należy oznaczyć nagłówkami odpowiedniego poziomu.

12. Nagłówki dla redaktorów

Redaktorom należy zapewnić możliwość ustawiania odpowiedniej struktury nagłówkowej stron. Nagłówki dostępne dla redaktora powinny się zawierać od **h2** do **h6**. Nagłówek **h1** powinien najtrafniej opisywać główną treść strony.

13. Linki

W serwisie wszystkie linki powinny być zrozumiałe poza kontekstem tekstowym bądź wizualnym. W stałych częściach serwisu może oznaczać to potrzebę uzupełniania krótkich linków o treści uzupełniające. Linki powinny być uzupełniane przez treści niewidoczne dla użytkowników niekorzystających z czytników ekranu, na przykład za pomocą klasy zwyczajowo nazywanej **sr-only** lub **visually-hidden** referującej do reguły CSS zawierającej zestaw właściwości ukrywających zawartość wyłącznie wizualnie.

Przykłady linków, które będzie można uzupełnić o dodatkową treść, to: zamknij, przewiń, następny, poprzedni, więcej, pobierz, pokaż wszystkie, itp.

14. Wielkość elementów interaktywnych

Wszystkie elementy interaktywne (np. przyciski, linki, ikony pola formularzy, elementy menu, itp.) muszą posiadać obszar klikalny o minimalnych wymiarach 24 x 24 piksele CSS. W wersji mobilnej oraz na urządzeniach dotykowych wszystkie te elementy muszą być rozmieszczone w sposób zapewniający łatwą aktywację jednym palcem, bez ryzyka przypadkowego użycia sąsiedniego elementu. Szczegółowe zasady oraz wyjątki opisuje kryterium 2.5.8 WCAG 2.2.

15. Teksty alternatywne

Wszystkie grafiki zamieszczone w szablonach za pomocą znacznika <img> muszą mieć atrybut alt.

1. W przypadku, gdy grafika nie będzie przekazywać żadnej treści (grafiki dekoracyjne), należy ją umieszczać za pomocą CSS, czyli stosując właściwość **background-image**. Inną metodą jest dodanie do **<img>** - pustego alt— zapis **alt** lub **alt="".**
2. Jeśli grafika będzie przekazywać treść, atrybut alt trzeba uzupełnić o adekwatny opis.
3. Jeśli grafika będzie jedyną zawartością linku, to w jej tekście alternatywnym należy przekazać cel linku. Jeśli link poza grafiką będzie zawierał tekst z informacją o jego celu (np. tekst widoczny, tekst ukryty wizualnie, ale dostępny dla czytników ekranu, **aria-label**), należy użyć pustego **alt**.

4. Elementy, które zostaną zaimplementowane za pomocą SVG muszą posiadać znacznik **<title> </title>,** w którym należy umieścić tekst alternatywny lub też dodać atrybut **aria-hidden="true**", jeśli ma to być grafika dekoracyjna.

16. Formularze — semantyka

Budowa formularzy pod względem dostępności musi opierać się o dobre praktyki HTML5. Należy uwzględnić, że formularze mogą być używane przez osoby z niepełnosprawnością wzroku, niepełnosprawne ruchowo czy głucho-niewidome, np. bez użycia myszki czy bez patrzenia na ekran.

W większości przypadków jako podstawy semantyki HTML dla formularzy rozumie się:

1. użycie etykiet do wszystkich pól (etykiety muszą być widoczne),
2. zrozumiałość etykiet,
3. dostęp do wszelkich wskazówek bez konieczności patrzenia na ekran, np. za pośrednictwem czytnika ekranu,
4. kolejność treści i pól formularzy wspierająca użyteczność i zrozumiałość,
5. zdefiniowanie atrybutu “autocomplete”,
6. umożliwienie ponownego użycia wcześniej wprowadzonych danych,
7. zachowanie minimalnego rozmiaru obszaru aktywnego elementów interaktywnych, co najmniej 24 × 24 piksele CSS, zgodnie z kryterium 2.5.8 WCAG 2.2.
8. zdefiniowanie wymagalności pól (aria-required=”true/false” or required).

Etykiety powinny być programistycznie powiązane z polami formularzy za pomocą atrybutów **for i id.**

Dodatkowe informacje, które ułatwią użytkownikowi wypełnić formularz powinny być powiązane z elementem **<input>** za pomocą atrybutu **aria-describedby**.

W przypadku serwisów, w których użytkownik wypełnia dane osobowe inne niż swoje, **autocomplete** powinien zostać ustawiony na wartość **off**. Wówczas przeglądarka nie będzie podpowiadała użytkownikowi jego osobistych danych. Brak takiego atrybutu może spowodować, że przeglądarka będzie szukała tych wartości domyślnie.

W sytuacji, gdy formularz służy do wprowadzenia własnych danych użytkownika, wówczas atrybut **autocomplete** powinien przyjąć konkretną wartość tak jak na przykład:

- Imię: **given-name**
- Nazwisko: **family-name**
- Adres e-mail: **email**
- Telefon: **tel**
- itd.

Pozostałe wartości atrybutu **autocomplete**.

17. Formularze — wsparcie użytkownika i informacja o błędach

Informacje o błędach powinny być prezentowane tekstowo, bezpośrednio przy polach, których dotyczą (dodatkowo powiązane z polem poprzez **aria-describedby**) oraz pod

nagłówkiem rozpoczynającym blok z formularzem. Powinien istnieć jeden, ogólny komunikat informujący użytkownika o błędnym wypełnieniu formularza wraz z rolą alert. Szczegóły takiego rozwiązania znajdują się na stronie Techniques for WCAG.

Błędnie wypełnione pole formularza należy oznaczyć atrybutem **aria-invalid="true"**.

W tym przypadku należy kierować się następującym podejściem:

1. Wszystko, co możliwe, należy wykonać za pomocą podstawowych elementów HTML + JavaScript — im dalej będzie sięgać wsteczna kompatybilność, tym lepiej,
2. Jeśli formularz będzie tego wymagał, należy zastosować atrybuty ARIA.

Kolejność w powyższym wypunktowaniu jest ważna - użytkownicy mogą korzystać z przestarzałego oprogramowania, dlatego trzeba zagwarantować wsteczną kompatybilność w jak największym stopniu.

Formularze muszą umożliwiać automatyczne uzupełnienia danych, które system już zna, lub które użytkownik wcześniej wprowadził w ramach bieżącej sesji.

18. Tabele

W przypadku tabel, kluczowe jest stosowanie odpowiedniej składni i semantyki HTML. Czytniki ekranu wspierają obsługę tabel bardzo dobrze.

Tabele z danymi muszą mieć prawidłowo zdefiniowane semantycznie wiersze/kolumny nagłówkowe. Prawidłowa implementacja jest kluczowa dla zrozumienia tabeli przez narzędzia asystujące.

Należy zwrócić szczególną uwagę na informowanie technologii asystującej na temat stanu sortowania/filtrowania oraz ilości danych w tabeli.

Wskazówki, które pomogą w tworzeniu dostępnych tabel, znajdują na stronie konsorcjum w3.org.

19. Działanie Systemu za pomocą klawiatury

Prawidłowe zastosowanie semantyki HTML musi gwarantować dostępność za pomocą klawiatury każdego aktywnego elementu na stronie

Jeśli programiści muszą stosować zarządzanie fokusem przez JavaScript, to należy robić to w taki sposób, aby nie stworzyć tzw. pułapki klawiaturowej. Taki błąd powoduje barierę dla użytkowników z niepełnosprawnością ruchu oraz korzystających z czytników ekranu.

20. Ruchy przeciągania

Wszelkie funkcje, które w Systemie wymagają wykonania ruchu przeciągania (np. „przeciągnij i upuść” element, suwak, sortowanie listy, przesuwanie kart, zmiana położenia elementu itp.), muszą mieć zapewnioną równie skuteczną alternatywę, niewymagającą przeciągania.

Przykłady alternatywnych rozwiązań:

1. przyciski „przenieś w górę / w dół”,
2. przyciski „lewo / prawo” do przesuwania elementów,

3. możliwość zmiany pozycji elementów za pomocą klawiatury,
4. użycie przycisków potwierdzenia (np. „Wybierz element”, „Przenieś tutaj”) zamiast przeciągania.

Alternatywa musi być w pełni dostępna z poziomu klawiatury oraz współpracować z technologiami asystującymi.

21. Kolejność fokusu

Fokus klawiatury musi mieć kolejność wedle reguły od lewej do prawej i od góry do dołu. Komponenty powinny przyjmować fokus w kolejności, dzięki której zachowany jest sens i funkcjonalność treści. Na przykład, po przejściu fokusem menu głównego, powinien on trafić do głównego bloku treści lub lewej kolumny.

22. Ukrywanie treści

W niektórych przypadkach, np. w linkach, może być konieczne stosowanie ukrytej treści. Takie rozwiązanie wspiera korzystanie z Systemu przez użytkowników z niepełnosprawnością wzroku.

Artykuły opisujące techniki ukrywania treści:

1. Techniki ukrywania treści - artykuł na stronie webaim.org.
2. Techniki ukrywania treści - artykuł na stronie getbootstrap.com.

Poza tymi obszarami, w których Wykonawca zaproponuje użycie techniki ukrywania, w ramach monitoringu wdrożenia, ekspert ds. dostępności ze strony Zamawiającego pracujący w ramach zespołu projektowego wskaże ewentualne dodatkowe miejsca, w których należy zastosować tę technikę.

23. Dostępne zabezpieczanie formularzy i uwierzytelnianie

System musi stosować mechanizmy zabezpieczania formularzy, procesów logowania, autoryzacji oraz odzyskiwania dostępu w sposób, który **nie stwarza barier dostępności**, w szczególności dla osób z niepełnosprawnościami oraz osób z trudnościami poznawczymi.

Zabezpieczenia nie mogą wymagać od użytkownika zapamiętywania, rozpoznawania ani przepisywania złożonych informacji.

Preferowane są mechanizmy niewymagające dodatkowych działań po stronie użytkownika (np. filtrowanie po stronie serwera, analiza behawioralna, limity żądań).

System nie może wymagać od użytkownika:

1. zapamiętywania złożonych haseł lub sekwencji znaków bez wsparcia mechanizmów ułatwiających (np. menedżery haseł),
2. rozwiązywania zagadek wizualnych lub dźwiękowych (np. CAPTCHA),
3. rozpoznawania obrazków, symboli, dźwięków lub zniekształconych tekstów jako formy potwierdzenia tożsamości lub zabezpieczenia formularza.

CAPTCHA i mechanizmy równoważne:

1. Stosowanie CAPTCHA jest co do zasady **niedozwolone**, chyba że oferuje pełnowartościową, równorzędną alternatywę dostępną dla wszystkich użytkowników.
2. Proste mechanizmy typu „Nie jestem robotem” nie są uznawane za dostępne, jeżeli nie zapewniają pełnej obsługi z klawiatury oraz przez technologie asystujące.
3. Każde zastosowanie CAPTCHA lub mechanizmu podobnego będzie podlegało szczegółowej weryfikacji pod kątem dostępności.

Dopuszczalne metody uwierzytelniania
System musi oferować co najmniej jedną metodę uwierzytelnienia dostępną poznawczo, w szczególności:

1. logowanie przy użyciu zapisanych poświadczeń przeglądarki,
2. uwierzytelnianie poprzez link lub kod jednorazowy przesyłany e-mailem lub SMS,
3. logowanie przez zewnętrzne, dostępne systemy (np. login.gov.pl, ePUAP, OAuth),
4. możliwość wklejenia danych lub kodów bez konieczności ich przepisywania.

Jeżeli z przyczyn bezpieczeństwa stosowane są dodatkowe mechanizmy (np. 2FA), muszą one być możliwe do wykonania:

1. bez użycia wzroku i słuchu,
2. bez złożonych gestów,
3. bez konieczności skomplikowanego rozumowania.

24. Działanie filtrów/przeładowanie
Wszelkie działania związane z przeładowaniem widoku takie jak:

1. filtrowanie,
2. sortowanie,
3. wyszukiwanie,

należy przetestować z czytnikami ekranu. W takich sytuacjach kluczowy będzie komfort obsługi bezwzrokowej. Użytkownik powinien mieć pełną wiedzę na temat działania interfejsu i świadomość tego, że treść strony została zaktualizowana.

Zamawiający dopuści zmiany treści strony bez przeładowania tylko w uzasadnionych sytuacjach.

W niektórych przypadkach, po zmianie przefiltrowania może być konieczna automatyczna zmiana tytułu strony **<title>**.

25. Elementy rozwijane
Wszystkim interaktywnym elementom, które umożliwiają rozwijanie i zwijanie kontrolowanych przez siebie komponentów (np. przycisk rozwijający menu nawigacyjne) należy przypisać atrybut **aria-expanded**. Jego wartość należy ustawić z poziomu JS (**true** albo **false**) - w zależności czy kontrolowany przez niego komponent jest zwinięty czy rozwinięty: **aria-expanded="true"** jeśli jest rozwinięty, **aria-expanded="false"** jeśli jest zwinięty. Dzięki

temu użytkownicy korzystający z aplikacji asystujących będą wiedzieli jaka jest aktualna struktura zamieszczonych informacji.

26. Elementy zmienne

Wszelkie elementy, które zmieniają swoją wartość, dzięki działaniu jakiegoś mechanizmu (na przykład kalkulatora czy formularza), muszą mieć atrybut **aria-live**. Dzięki niemu użytkownik jest informowany o zmianie treści na stronie. Przykłady działania atrybutu aria-live znajdują się na stronie Deque University.

27. Działanie z mechanizmami służącymi zwiększaniu czytelności treści

System musi bezproblemowo działać ze zintegrowanymi z systemami operacyjnymi mechanizmami służącymi zwiększaniu czytelności treści. Przykładami takich mechanizmów jest tryb dużego kontrastu w systemie Windows czy odwrócenie kolorów w systemach macOS/iOS. Wykonawca powinien prowadzić takie testy na bieżąco w trakcie wdrożenia.

Typowe problemy w takim trybie mogą być związane z użyciem CSS-owego zastępowania tekstu grafiką. Dlatego w niektórych przypadkach zamiast użycia takiej techniki, będzie konieczne zastosowanie typowych linków graficznych **<a><img>**.

28. Skip linki

Na każdej stronie serwisu powinien działać link „**Przejdź do wyszukiwania**”, „**Przejdź do głównej treści**” (jeżeli takie elementy występują), które pomagają przeskoczyć fokusem bezpośrednio do głównej funkcjonalności danej strony. Najczęściej będzie to oznaczać ominięcie nawigacji lub też innych powtarzających się elementów na stronie. Nie zaleca się stosowania więcej niż trzech skip linków. Takie elementy należy zaprojektować i skonsultować z Zamawiającym.

8. Inne wymagania techniczne

29. Szybkość działania Systemu SOF2

System SOF2 musi być maksymalnie zoptymalizowany do szybkiego działania. Lekkość serwisu wpływa pozytywnie na działanie z oprogramowaniem wspomagającym, takim jak na przykład czytnik ekranu. Powoduje również komfortową obsługę w urządzeniach mobilnych. W ramach optymalizacji pod kątem szybkości działania trzeba będzie zwrócić uwagę na następujące kwestie:

1. brak nadmiarowego kodu HTML/CSS/JS;
2. nieobciążanie Systemu zbędnymi dodatkami JS;
3. dobrą optymalizację grafiki;
4. minimalizację liczby plików pobieranych wraz z unikalną stroną;
5. cache serwisu, który zminimalizuje zapytania do bazy danych.

30. Responsywność (RWD)

Przy budowaniu serwisu należy pamiętać o urządzeniach mobilnych, które pełnią ważną rolę w odbiorze treści internetowych.

Serwis należy zbudować w oparciu o najlepsze i aktualne praktyki tworzenia serwisów responsywnych (np. media queries, container queries, grid, flexbox).

Wszystkie projekty graficzne muszą być przygotowane z zastosowaniem skoków responsywnych szerokości w odniesieniu do typów urządzeń (standardów):

1) smartfon;
2) tablet;
3) monitor komputerowy.

Obiekty nie mogą zachodzić na siebie i przykrywać treści, bądź funkcjonalności.

Przy projektowaniu widoków mobilnych należy uwzględnić minimalną wielkość fontów – 16 px. Jest to wartość ważna podczas analizy czytelności strony.

31. Możliwości edytora WYSIWYG

W edytorze wizualnym poza standardowymi funkcjami, należy udostępnić redaktorom kilka dodatkowych narzędzi. Dokonując wyboru **WYSIWYG** trzeba będzie sprawdzić, czy rozwiązanie obsługuje dane funkcje natywnie, np. na podstawie pluginów.

Wstępna rekomendacja na rozwiązanie WYSIWYG to TinyMCE.

32. Działanie z oprogramowaniem wspomagającym

Działanie Systemu będzie analizowane przy użyciu:

- popularnych czytników ekranu — NVDA, JAWS, VoiceOver;
- powiększalników takich jak ZoomText;
- trybu wysokiego kontrastu Windows;
- urządzeń typu switch;
- urządzeń mobilnych z systemami Android / iOS, a w tych systemach z:
    - czytnikami ekranu;
    - rozwiązaniami typu switch;
    - powiększaniem ekranu i tekstu.

Testy zostaną przeprowadzone zarówno przez ekspertów jak i z użytkownikami z niepełnosprawnościami.

9. Wytyczne dostępności (graficzne)

33. Kontrast treści

Kontrast między kolorem tekstu a kolorem jego tła, musi wynosić minimum 4,5:1 lub 3:1 dla tekstu o wielkości co najmniej 24 px (bez pogrubienia) lub 18 px dla tekstu pogrubionego. większego tekstu (krój pisma pogrubiony o przybliżonej wielkości powyżej 18 px, lub 24px lub większy).

Prostym narzędziem do analizy poziomu kontrastu jest Colour Contrast Analyzer.

W związku z wymogami dotyczącymi kontrastu, nie powinieneś stosować elementów prezentujących tekst na tle niejednorodnym, np. bezpośrednio na tle zdjęcia. Istnieje jednak wiele technik umożliwiających podniesienie kontrastu takiego tekstu. Przykładowo, w przypadku białego tekstu na tle zdjęcia z dużymi obszarami jasnych kolorów, można

przypisać do samego tekstu częściowo przezroczyste tło w kolorze kontrastującym względem tekstu, czyli w tym przypadku czarnym:

```
.bgtext {
  color: rgb(255 255 255);
  background-color: rgb(0 0 0 / 70%);
  padding: 1em;
}
```

Możesz stosować kolorystykę o mniejszym kontraście, ale tylko w zakresie elementów dekoracyjnych w serwisie. Kryterium kontrastu nie obejmuje logo serwisu/systemu.

34. Identyfikacja linków

Linki tekstowe muszą być łatwe do odnalezienia przez wszystkich użytkowników serwisu.

Muszą odróżniać się od tekstu zarówno kolorem jak i podkreśleniem. Niedopuszczalne jest zastosowanie tylko koloru do wyróżnienia linku.

Podkreślenia mogą być użyte w projekcie graficznym wyłącznie do oznaczenia linków. To samo dotyczy koloru linków. Nie może być on powtórzony na żadnym elemencie nieklikalnym i musi spełniać wymogi wskazane w punkcie “Kontrast treści”.

Po umieszczeniu na linku kursora myszy (**hover**) powinien on wizualnie odróżniać się od pozostałych linków, przy czym odróżnienie to nie powinno opierać się wyłącznie na kolorze (np. podkreślenie linku powinno znikać, a kolor linku zmieniać się na kolor o wyższym wskaźniku kontrastu do tła, niż przy kolorze bazowym linku).

35. Formularze

Wymóg widoczności dotyczy również formularzy stosowanych w serwisie. W szczególności odnosi się to do widoczności ramek pól, etykiet pól oraz przycisków.

Wszystkie elementy formularzy (między innymi kolor ramek pól edycyjnych, elementy przycisków radiowych czy ramek przycisków do zaznaczenia – checkbox) muszą spełniać wymóg minimalnego kontrastu w stosunku do tła na poziomie przynajmniej 3:1.

Tak jak w przypadku linków, przyciski formularzy po umieszczeniu na nich kursora myszy muszą stawać się widoczne dla użytkowników (np. zwiększenie kontrastu między kolorem przycisku, a kolorem tekstu przycisku).

36. Fokus klawiatury

Cały serwis musi umożliwiać nawigację za pomocą samej klawiatury.

Fokus klawiatury musi mieć formę wzmocnioną w stosunku do fokusu domyślnego przeglądarki i być widoczny przy nawigacji za pomocą klawiatury w formie ramki, wokół wybranego elementu.

Kolor ramki fokusu musi być dobrany do schematu kolorystycznego serwisu tak, aby był dobrze widoczny na oznaczonym elemencie (minimalny kontrast – 3:1).

Element interfejsu użytkownika, który otrzymuje fokus klawiatury, nie może być całkowicie zasłonięty przez inne elementy strony (np. przyklejone nagłówki, banery, modale, panele pływające).

W przypadku automatycznego przewijania widoku fokusowany element musi być co najmniej częściowo widoczny.

Przykład dobrze widocznego fokusu możesz zobaczyć w serwisie www.pfron.org.pl – wystarczy zacząć nawigację w serwisie za pomocą przycisku TAB.

Do rozróżnienia fokusu myszy i klawiatury możesz wykorzystać pseudoklasy **:focus** oraz **:focus-visible**.

37. Typografia

Czcionki, użyte w Systemie muszą być bezszeryfowe, o wysokim poziomie czytelności - także przy dużym powiększeniu. Zamawiający dopuszcza zastosowanie czcionek typu: Lato, Open Sans czy PT Sans.

Liczba czcionek (krój i wielkość) musi być ograniczona w projekcie graficznym serwisu do niezbędnego minimum.

38. Spójna identyfikacja

W ramach Systemu należy zaplanować widoki tekstowych elementów semantycznych, takich jak:

1. nagłówek poziomu 1, (każda strona musi posiadać jeden nagłówek poziomu 1, pozostałe w odpowiedniej hierarchii, jeżeli treść jest wymagana.
2. lista numerowana (uporządkowana),
3. lista wypunktowana (nieuporządkowana),
4. listy obu typów wielokrotnie zagnieżdżone,
5. link,
6. tekst podstawowy,
7. tekst podstawowy wyróżniony,
8. przycisk (3 schematy dla różnych funkcjonalności),
9. listy rozwijane (select),
10. przyciski typu radio,
11. pola wyboru,
12. pole edycyjne.

Wielkość krojów pisma użytych w poszczególnych stylach ma odpowiadać hierarchii tych stylów względem siebie. Należy przyjąć zasadę, że nagłówek poziomu 6 ma być co najmniej wielkości kroju pisma podstawowego, tylko pogrubionego.

Minimalna wielkość kroju pisma, którą Zamawiający dopuszcza w projekcie graficznym to 12 px., przy czym treść podstawowa musi mieć wielkość minimum 16 px.

Nie należy stosować wersalików – wielkich liter do treści.

Odstępy między wierszami w akapitach ma być ustawiony na co najmniej 1,3-1,5 wysokości linii, a odległość między akapitami na przynajmniej 1,5 razy większą niż ta pomiędzy wierszami. W innym przypadku Wykonawca zapewni możliwość zmiany wielkości, bez utraty treści (np. za pomocą 1.4.12 Text Spacing – narzędzie wspomagające symulację strony ze zwiększonymi odstępami w zakresie podanym w WCAG 2.2.)

W jednym wersie można zaprezentować do 80 znaków.

Zamawiający nie dopuszcza możliwości justowania (równoczesne wyrównanie do lewej i prawej) żadnej treści w projekcie graficznym. Dopuszcza tylko wyrównanie do lewej, a w uzasadnionych sytuacjach wyśrodkowanie tekstu.

Tam, gdzie to możliwe, treść ma być zaprezentowana w formie tekstu, a nie grafiki tekstu. Do osiągnięcia pożądanego wyglądu Wykonawca użyje odpowiednich stylów CSS.

System SOW ma być spójny pod względem zarówno w zakresie użycia krojów pisma lub stylów, jak i jednolitej implementacji tych samych elementów na różnych podstronach, np. ten sam opis logo Systemu we wszystkich miejscach, w których występuje bądź też elementu ukazującego podpowiedź przy wypełnianiu formularza (nie może raz być to “otwórz podpowiedź”, a za innym razem “pomoc”).

39. Spójna pomoc

Wszystkie elementy wsparcia użytkownika (np. link „Pomoc”, kontakt do administratora, czat, FAQ, formularz kontaktowy, itd.) muszą być umieszczone w tym samym spójnym miejscu interfejsu. Użytkownik musi zawsze wiedzieć, gdzie na stronie znajdzie element pomocy, bez konieczności ponownego jej poszukiwania.

Spójność dotyczy zarówno położenia elementu jak i sposobu jego opisania. Jeżeli serwis będzie zawierał wiele form pomocy, każda z nich musi być dostępna w przewidywalny sposób, a użytkownik musi mieć możliwość wyboru preferowanej metody pomocy.

40. Tabele

Tabele z danymi prezentowane w projekcie graficznym muszą posiadać wyraźnie odróżniające się od reszty komórek wersy/kolumny nagłówkowe. Komórki tabeli powinny zostać rozdzielone krawędziami o kolorze zapewniającym minimalny kontrast na poziomie 3:1.

41. Możliwość swobodnej zmiany wielkości widoku

Obsługa Systemu zakłada możliwość swobodnej zmiany wielkości strony (Ctrl + oraz Ctrl -). Należy upewnić się, że atrybut **content** elementu **<meta name="viewport">** nie zwiera parametrów blokujących możliwość powiększania takich jak **user-salable=no** czy **maximum-scale=1**. Przy każdej szerokości ekranu/poziomie powiększenia (nie tylko przeznaczonej dla tabletów i smartfonów) wszystkie treści i funkcje serwisu muszą być czytelne. Projekt graficzny musi umożliwiać zaprogramowanie w ten sposób serwisu.

42. Elementy ruchome

Dopuszczamy elementy ruchome w serwisie, ale tylko w połączeniu z przyciskiem, który umożliwi użytkownikowi ich zatrzymanie i ponowne uruchomienie.

Zalecamy respektowanie ustawienia systemowego prefers-reduced-motion, które sygnalizuje, że użytkownik preferuje ograniczenie animacji. Dzięki temu możliwe jest spełnienie wymagań wynikających z kryterium 2.3.3 WCAG (kryterium 2.3.3 Animacja po interakcji AAA) oraz dostosowanie serwisu do potrzeb użytkowników wrażliwych na ruch.

Technika W3C do zrealizowania tego kryterium – C39.

Żaden element serwisu nie może migać, jeśli czynność ta powtarza się więcej niż 3 razy na sekundę.

43. Multimedia

Jeżeli System będzie zawierał materiały wideo to rekomendujemy ich prezentację za pomocą standardowego odtwarzacza YouTube. Treści wideo muszą posiadać napisy i audiodeskrypcję. Projekt graficzny musi uwzględniać zamieszczanie bezpośrednio pod materiałem wideo linku do transkrypcji tekstowej materiału, jeśli nie jest umieszczona bezpośrednio w filmie.

10. Zalecenia na poziomie AAA

Interfejs graficzny Systemu SOF2 ma być zgodny z wytycznymi WCAG 2.2 poziomu A oraz AA. Dla wskazanych poniżej elementów interfejsu Wykonawca spełni zalecenia na poziomie AAA:

1. Kryterium sukcesu 2.4.9 Cel linku (poza kontekstem). Cel każdego odnośnika powinien być jednoznacznie określony również wtedy, gdy link jest odczytywany niezależnie od otaczającego go tekstu;
2. Kryterium sukcesu 1.4.8 Prezentacja wizualna:
    a. maksymalna szerokość linii tekstu nie przekracza 80 znaków;
    b. tekst nie jest wyjustowany (tzn. wyrównany do prawego i lewego marginesu);
    c. tekst powiększony do 200% nie wymaga przesuwania w poziomie.
3. Kryterium sukcesu 2.3.3 Animacja po interakcji. Animacje wywoływane przez interakcję użytkownika mogą zostać wyłączone, aby uniknąć rozpraszania lub dyskomfortu.

11. Dokumenty

Wszystkie dokumenty, publikowane w Systemie SOF2 , muszą spełniać wymagania WCAG w odniesieniu do dokumentów cyfrowych (zalecenia w tym zakresie dostępne są na stronie W3C, która opisuje techniki WCAG dla PDF).

Wykonawca jest zobowiązany do każdorazowej adaptacji dokumentów dostarczanych przez zamawiającego oraz prawidłowego (zgodnego z wytycznymi WCAG) przygotowania Dokumentacji Użytkownika.

Dokumentacja Użytkownika musi być przygotowana zgodnie z zasadami prostego języka umieszczonymi w serwisie gov.pl.

12. Weryfikacja stosowania wytycznych

Zamawiający zastrzega sobie prawo do weryfikacji serwisu, w każdy dostępny sposób, pod względem zgodności ze specyfikacjami W3C. Zakres weryfikacji może dotyczyć:

- zgodności z kryteriami WCAG,
- prawidłowego stosowania technik dla WCAG,
- zgodności specyfikacji ARIA.

Możliwość weryfikacji dotyczy całego okresu obowiązywania Umowy. W przypadku stwierdzenia jakiekolwiek niezgodności Wykonawca będzie zobowiązany do ich usunięcia na własny koszt w terminie wskazanym przez zamawiającego.

Załącznik nr 3 do OPZ - Wymagania dla Dokumentacji.

1. **Wymagania Ogólne**

DOK-1. W terminie 10 Dni Roboczych od uzyskania dostępu do Repozytorium Projektowego, Wykonawca zapozna się z dokumentacją i sposobem organizacji i zarządzania Repozytorium Projektowego oraz przedstawi Zamawiającemu propozycje optymalizacji ww. Repozytorium. Zamawiający zastrzega sobie prawo do wyboru poszczególnych propozycji przedstawionych przez Wykonawcę.

DOK-2. Wykonawca w terminie 10 Dni Roboczych następnego dnia od dnia zaakceptowania przez Zamawiającego propozycji optymalizacji Repozytorium Projektowego wprowadzi je do Repozytorium.

DOK-3. Wykonawca zobowiązuje się do prowadzenia Repozytorium Projektowego w oparciu o środowisko dostarczone przez Zamawiającego. Środowisko zostanie skonfigurowane we wskazany przez Zamawiającego sposób, na wskazanej przez Zamawiającego infrastrukturze z wykorzystaniem wskazanego przez Zamawiającego środowiska systemu kontroli wersji (GIT), narzędziu typu case-tracker na przykład JIRA, narzędzia pracy grupowej na przykład Microsoft Teams, Sharepoint.

DOK-4. W Repozytorium Projektowym, w sposób szczególny będą wyróżniane aktualne wersje dokumentacji projektowej. Dokumenty projektowe będą zawierały historię zmian oraz dane identyfikacyjne, w tym numer wersji.

DOK-5. Wykonawca odpowiedzialny jest za sporządzanie notatek ze spotkań projektowych i umieszczanie ich w Repozytorium Projektowym.

DOK-6. Wykonawca zobowiązany jest do utworzenia dokumentu dotyczącego planu odtworzenia Systemu po awarii (Disaster Recovery Plan).

DOK-7. Wykonawca sporządzi instrukcję zawierającą procedurę wykonania kopii bazy danych Systemu oraz jej odtworzenia. Dokument powinien również dotyczyć tworzenia i przywracania bazy danych z serwera produkcyjnego na serwer testowy Systemu.

DOK-8. Repozytorium architektury będzie m.in. służyć jako źródło do generowania części lub całości Dokumentacji Systemu omawianej w niniejszym Załączniku. Repozytorium architektury musi być prowadzone w narzędziu Sparx Enterprise Architect w wersji co najmniej 14.

2. Organizacja, formatowanie, komentowanie i utrzymanie Kodu Źródłowego.

2.1. Przechowywanie Kodu Źródłowego.

2.1.1. Repozytorium Kodu Źródłowego

Zamawiający prowadzi i nadzoruje Repozytorium Kodu Źródłowego. W przypadku projektów realizowanych przez firmy trzecie, pracownicy tych firm są odpowiedzialni za zarządzanie projektem i Kodem Źródłowym w repozytorium. W przypadku prac wykonywanych przez pracowników PFRON, taki obowiązek leży po stronie Funduszu. Repozytorium Kodu Źródłowego oparte jest na platformie GIT z wykorzystaniem interfejsu graficznego GitLab. Zasady korzystania i prowadzenia repozytorium kodu źródłowego określają poniższe zapisy:

a) Każdy realizowany w PFRON projekt musi posiadać własną przestrzeń w systemie GitLab, tzw. projekt.
b) Projekt w GitLab musi mieć nazwę zgodną z nazwą projektu realizowanego w organizacji.
c) Kody źródłowe przekazywane są w formie zapewniającej kontrolę wersji.
d) Repozytorium kodu nie powinno być traktowane jako archiwum, wymagane jest ciągłe dostarczanie kolejnych wersji Kodu Źródłowego, zgodnie z procesem wytwórczym. Nie akceptowalna jest forma rzadkiego zatwierdzania commitów z dużą ilością linii Kodu Źródłowego.
e) W przypadku gdy, do aplikacji wykorzystane zostały Kody Źródłowe lub biblioteki innych dostawców a następnie zostały one zmodyfikowane na potrzeby projektu, bezwzględnie należy dodać do repozytorium kod wejściowy biblioteki lub modułu, a następnie wersjonować realizowane w nim zmiany.
f) Każdy commit powinien zawierać ogólny opis (jakiej funkcjonalności, pakietu dotyczy, do czego służy, dlaczego coś było modyfikowane - zmieniane) zmian oraz autora i wersję systemu, którego dotyczy.
g) Każdy commit powinien zawierać również informacje umożliwiające łatwe powiązanie poszczególnych aktualizacji Repozytorium Kodu Źródłowego z dokumentacją projektu, w tym dokumentacją zmian i dokumentacją Kodu Źródłowego.

2.1.2 Organizacja Repozytorium Kodu Źródłowego.

Struktura repozytorium powinna posiadać podział na moduły aplikacji, usługi integracyjne, konfiguracje i pliki specyficzne dla środowisk, strukturę bazy danych oraz obiekty bazodanowe, w tym pakiety, procedury, funkcje, wyzwalacze.
Strategia tworzenia gałęzi (ang. Branching Strategy) w narzędziu GitLab powinna być zgodna z zasadami GitFlow (https://datasift.github.io/gitflow/IntroducingGitFlow.html). Główną gałęzią musi być *master*. Bieżące prace rozwojowe powinny być prowadzone w oddzielnej gałęzi, na przykład o nazwie *develop*. Wytwarzanie pojedynczych nowych funkcjonalności w ramach prac rozwojowych odbywać się powinno w gałęziach *feature* (ang. feature branches). Prace programistyczne związane z usuwaniem błędów prowadzone są na osobnej gałęzi, na przykład *HotFIX*. Po zakończeniu prac rozwojowych lub utrzymaniowych i

wdrożeniu zmian na środowisko produkcyjne danego systemu kod źródłowy z odpowiedniej gałęzi musi być połączony z gałęzią *master*.

2.2. Komentowanie Kodu Źródłowego.

2.2.1. Konwencja nazewnictwa.

Projekty realizowane w PFRON muszą posiadać opracowaną i stosowaną w ramach danego projektu konwencję nazewniczą. Konwencja musi zapewnić minimum:

a) Usystematyzowanie, uporządkowanie i ujednolicenie nazewnictwa w ramach danego projektu.
b) Umożliwiać łatwe rozróżnianie (po nazwie) typu zmiennej, stałej, kolumny w bazie, wartości zwracanej przez funkcję, metodę itp.
c) Nazwy mają być znaczące - informować o tym, do czego dany element jest wykorzystywany.
d) Konwencja powinna być opracowana i opisana w taki sposób, by programista pisząc kod nie miał wątpliwości jakich nazw ma używać.
e) Konwencja powinna uwzględniać instalacje testowe, tak aby nie wprowadzać chaosu pomiędzy np. nazwami/identyfikatorami elementów systemu dla instalacji testowej i produkcyjnej.

Opracowana konwencja nazewnicza musi uwzględniać minimum następujące elementy i twory programistyczne:

a) Wszystkie elementy Kodu Źródłowego, w tym pakiety, biblioteki, klasy, metody, pola klas, stałe, zmienne, funkcje, procedury itp.
b) Wszystkie składniki systemu baz danych, w tym nazwa baza danych, nazwy schematów, tabele, kolumny, funkcja, pakiet, wyzwalacz, tabele tymczasowe, zmienne itp.
c) Innych składników systemu, takich jak API, zmiennych formatu XML oraz JSON itp.

Nazwy obiektów programistycznych i bazodanowych, w tym nazwy zmiennych, metod, klas muszą być intuicyjne, jednoznaczne i napisane w języku polskim. W przypadku gdy nazwy będą zapisywane w języku angielskim, ich polskie odpowiedniki muszą być zapisywane w komentarzu związanym z danym obiektem programistycznym lub bazodanowym. W przypadku nazw klas, metod, zmiennych, funkcji, obiektów bazodanowych (tabele, kolumny, procedury, funkcje, zmienne itp.) należy obowiązkowo unikać nazw jednoliterowych oraz skrótów zrozumiałych w danym momencie wyłącznie dla programisty piszącego dany kod. Wyjątkiem od powyższych zasad jest kod źródłowy bibliotek i frameworków wytworzonych przez firmy trzecie i wykorzystywanych w ramach danego projektu. W przypadku modyfikacji ww. bibliotek lub frameworków, zmiany wprowadzone do kodu źródłowego muszą spełniać już wymagania opisane w niniejszym dokumencie.

2.3. Formatowanie Kodu Źródłowego.

Dla każdego projektu należy zdefiniować formatowanie Kodu Źródłowego. Wszyscy, biorący udział w projekcie programiści muszą obligatoryjnie stosować jednolite formatowanie.
Kod źródłowy musi spełniać wymagania dotyczące kodu samo komentującego, powinien być sformatowany w sposób prosty, przejrzysty oraz jednolity.

Przykłady standardów formatowania dla Kodu Źródłowego:

- JAVA -Google Java Style Guide (https://google.github.io/styleguide/javaguide.html)
- PHP – PSR PHP Standard Recommendations (https://www.php-fig.org/psr/)
- Python – PEP8 (https://www.python.org/dev/peps/pep-0008/)
- PostgreSQL – Coding Standard for SQL and PL/SQL (https://www.williamrobertson.net/documents/plsqlcodingstandards.html)

2.4. Komentowanie Kodu Źródłowego.

Sposób komentowania i jakość samych komentarzy ma bezpośrednie znaczenie dla jakości Kodu Źródłowego danego systemu.

Główna reguła, która musi być stosowana w przypadku konstruowania komentarzy do kodu źródłowego brzmi następująco: Należy komentować Kod Źródłowy w taki sposób, jakiego tworzący komentarz programista sam by oczekiwał - co do zakresu, podejścia, zawartości, szczegółowości, konsekwencji w stylu, spójności konwencji itd.

2.4.1. Minimalne wymagania dotyczące komentowania Kodu Źródłowego.

a) każda klasa (aplikacji, formularzy, raportów itd.) musi zawierać kilkuzdaniowy komentarz opisujący, jakiego rodzaju obiekty generuje i jaka jest ich semantyka,
b) każdy atrybut każdej klasy musi zawierać komentarz opisujący jego znaczenie,
c) każda metoda każdej klasy musi zawierać komentarz opisujący, do czego metoda służy, jakie ma parametry (co one oznaczają) oraz jaką wartość zwraca,
d) każde wywołanie metody obiektu musi zawierać komentarz objaśniający, czemu służy,
e) każde wykonanie instrukcji SQL musi zawierać komentarz objaśniający, czemu służy,
f) każda tabela oraz kolumna musi posiadać komentarz objaśniający jakie dane są przechowywane w danej tabeli lub kolumnie, jeśli sama nazwa nie posiada odpowiedniej informacji,
g) każdy obiekt bazodanowy, w tym, pakiet, funkcja, wyzwalacz itp. musi zawierać komentarz objaśniający, czemu służy.

Każdy obiekt programistyczny, taki jak pakiet, klasa, metoda, procedura, funkcja, pakiet bazodanowy, procedura bazodanowa, funkcja bazodanowa itp. zawiera opis nagłówkowy, zawierający przynajmniej poniższe informacje:

- autor,
- numer wersji obiektu,
- numer wersji systemu,
- data utworzenia i data ostatniej modyfikacji,
- lista i opis argumentów (jeśli takie posiada),
- opis zwracanej wartości (jeśli zwraca wartość) lub wyniku działania,

- krótki, ale wyczerpujący opis działania, słowny opis użytego algorytmu,
- zwracane nieobsłużone wyjątki (jeśli takie mogą się pojawić),
- ewentualnie odwołanie do dokumentacji systemu.

Komentarze wewnątrz pakietów, klas, procedur, funkcji, pakietów bazodanowych, procedur bazodanowych, funkcji bazodanowych itp. Muszą być umieszczone w przypadku, gdy:

- wyjaśnienie kodu, który nie jest oczywisty na pierwszy rzut oka,
- wyjaśnienie intencji, które ciężko ująć w kodzie,
- ostrzeżenie o konsekwencjach użycia danej funkcjonalności,
- wyjaśnienie niuansów procesów biznesowych, które realizuje program.

Komentarze Kodu Źródłowego należy uzupełniać o znaczniki wymagane przez narzędzia służące do automatycznego generowania dokumentacji Kodu Źródłowego wprost z plików źródłowych. W przypadku języka programowania PHP, komentarze powinny być opisane sposób pozwalający na wygenerowanie dokumentacji za pomocą narzędzia PHPDoc, phpDocumentor lub Doxygen. Dodatkowe wymagania dotyczące komentowania Kodu Źródłowego i znaczników interpretowanych przez dane narzędzie znajdują się w jego dokumentacji.

2.5. Dokumentacja Kodu Źródłowego.

Niezależnie od komentarzy znajdujących się w Kodzie Źródłowym i na tej podstawie wygenerowanej dokumentacji, wykonawcy realizujący projekty programistyczne w Funduszu zobligowani są do utworzenia, aktualizacji i prowadzenia dokumentacji kodu źródłowego. Dokumentacja, o której mowa powyżej musi zawierać:

a) wykaz (wraz z adresami w Git), całego Kodu Źródłowego koniecznego do generowania określonej wersji systemu. Do Kodu Źródłowego zalicza się również wszelkie dodatkowe zasoby takie jak skrypty, dane konfiguracyjne, frameworki itp.,
b) listę technologii wraz z wersją technologii, w których zostały wytworzone Kody Źródłowe. Dokumentacja musi być powiązana z konkretną wersją/wydaniem sytemu,
c) wygenerowaną automatycznie na podstawie Kodu Źródłowego, dokumentację Kodu Źródłowego przy użyciu wybranego dedykowanego narzędzia (np. javadoc). Dokumentacja jest pozyskiwana na podstawie odpowiednich znaczników wpisywanych w komentarze (o składni zgodnej z regułami narzędzia),
d) instrukcję generowania kodu wynikowego i tworzenia wersji instalacyjnej z wersji wynikowej (skompilowanej),
e) instrukcję konfiguracji środowiska do generowania kodów wynikowych,
f) specyfikację środowiska sprzętowo-systemowego wymaganego do przeprowadzenia procedury generacji kodu wynikowego,
g) listę narzędzi do przygotowywania wersji instalacyjnych wytworzonego oprogramowania (wersji pełnej, aktualizacji, łat) wraz z dokumentacją użytkowania i licencjami, o ile są wymagane,

h) w przypadku, gdy został wykorzystany framework firm trzecich, dokumentacja kodu źródłowego musi zawierać pełną dokumentację frameworka oraz instrukcję użytkownika i dla programistów,
i) w przypadku wykorzystania własnych standardowych bibliotek lub frameworków przez wykonawców dokumentacja kodu źródłowego musi również zawierać dokumentację ww. elementów systemu.

2.6. **Weryfikacja Kodu Źródłowego.**

2.6.1. Weryfikacja Kodu Źródłowego – wewnętrzna.

Częstotliwość weryfikacji Kodu Źródłowego – wymaganie ATK -12 (OPZ).
Weryfikacja Kodu Źródłowego będzie prowadzona dla:

a) Modyfikacji, wymuszających zmianę wersji systemu lub poszczególnych jego komponentów. Weryfikacja Kodu Źródłowego stanowić będzie część procedury odbioru modyfikacji i jej wynik końcowy ma wpływ na podpisanie lub nie protokołu odbioru.
b) Dostaw Kodu Źródłowego realizowanych w ramach umów usług utrzymania i rozwoju, zgodnie z określonymi w umowie terminami.
c) Dostarczonego Kodu Źródłowego nowo wytworzonego systemu, w ramach procedury odbioru.

W każdym przypadku osoby odpowiedzialne za realizację Umowy ustalają harmonogram oraz niezbędne zasoby osobowe i sprzętowe do przeprowadzenia weryfikacji. Weryfikację Kodu Źródłowego przeprowadzają pracownicy Zamawiającego i Wykonawcy w formie warsztatów. Wykonawca ma obowiązek zaprezentować wszystkie zmiany wprowadzone w kodzie w ramach realizacji usług ATiK i Rozwoju, w okresie, którego przegląd dotyczy.

2.6.2. Zakres wewnętrznej weryfikacji Kodu Źródłowego.

W celu zweryfikowania zgodności Kodu Źródłowego z wymaganiami zawartymi w niniejszym dokumencie należy przeanalizować Kod Źródłowy pod kątem poniższych zagadnień.

Lp.	Kryterium weryfikacji	Czy jest spełnione
1	Czy Kod Źródłowy jest przechowywany w GitLab?	Tak/Nie/Nie dotyczy
2	Czy projekt w GitLab ma nazwę zgodną z nazwą projektu?	Tak/Nie/Nie dotyczy
3	Czy sposób przechowywania Kodu Źródłowego zapewnia możliwość kontroli wersji?	Tak/Nie/Nie dotyczy
4	Czy commity wykonywane są z odpowiednią częstotliwością i są odpowiednio opisane?	Tak/Nie/Nie dotyczy
5	Czy Kod Źródłowy lub biblioteki innych dostawców znajdują się w GitLab?	Tak/Nie/Nie dotyczy

Lp.	Kryterium weryfikacji	Czy jest spełnione
6	Czy struktura repozytorium w GitLab jest odpowiednio przygotowana i adekwatna do projektu?	Tak/Nie/Nie dotyczy
7	Czy są tworzone i utrzymywane odpowiednie gałęzie w repozytorium GitLab?	Tak/Nie/Nie dotyczy
8	Czy projekt ma ustaloną konwencję nazewniczą?	Tak/Nie/Nie dotyczy
9	Czy konwencja nazewnicza jest stosowana w projekcie?	Tak/Nie/Nie dotyczy
10	Czy konwencja nazewnicza spełnia wymagania zawarte w dokumencie Standard komentowania Kodu Źródłowego?	Tak/Nie/Nie dotyczy
11	Czy w projekcie został zdefiniowany standard formatowania Kodu Źródłowego?	Tak/Nie/Nie dotyczy
12	Czy standard formatowania jest stosowany w projekcie?	Tak/Nie/Nie dotyczy
13	Czy kod źródłowy spełnia wymagania dotyczące samo komentującego?	Tak/Nie/Nie dotyczy
14	Czy komentarze zawarte w Kodzie Źródłowym spełniają minimalne wymagania zawarte w dokumencie Standard komentowania Kodu Źródłowego?	Tak/Nie/Nie dotyczy
15	Czy została wytworzona dokumentacja Kodu Źródłowego?	Tak/Nie/Nie dotyczy
16	Czy dokumentacja Kodu Źródłowego jest aktualna?	Tak/Nie/Nie dotyczy
17	Czy dokumentacja Kodu Źródłowego zawiera elementy wskazane w dokumencie Standard komentowania Kodu Źródłowego?	Tak/Nie/Nie dotyczy

Tab. 1 Lista kontrolna dla weryfikacji Kodu Źródłowego.

2.6.3. Weryfikacja Kodu Źródłowego – audyt zewnętrzny.

Na wniosek Kierownika Projektu lub innej osoby decyzyjnej weryfikacja Kodu Źródłowego może być przeprowadzona przez podmiot zewnętrzny.

Zakres audytu zewnętrznego będzie obejmować następujące obszary:

I. Obszar Kodu Źródłowego:
   a. Inspekcja kodu (code review) i wykorzystanie obowiązujących praktyk;
   b. Wykorzystanie przyjętych standardów komentowania i formatowania Kodu Źródłowego;

c. Wydajność Kodu Źródłowego i zapytań SQL;
d. Podatność na ataki;
e. Skalowalność Kodu Źródłowego;
f. Stopień odporności Kodu Źródłowego na wprowadzanie zmian, w tym refaktoryzację kodu (refactoring);
g. Zasięg i pokrycie testami automatycznymi;
h. Wykorzystane wzorce projektowe i poprawność ich użycia;
i. Optymalizacja i normalizacja bazy danych;
j. Ocena długu technologicznego;

II. Obszar procesu wytwórczego i zagadnień projektowych
a. Architektura aplikacji;
b. Wykorzystywana w projekcie technologia;
c. Poprawność wykorzystania frameworków i bibliotek;
d. Analiza potencjalnych kosztów wprowadzenia modyfikacji podczas fazy utrzymania i rozwoju systemu teleinformatycznego;
e. Jakość przyjętego w projekcie procesu wytwórczego.

Powyższy zakres audytu zewnętrznego Kodu Źródłowego będzie dostosowywany do indywidualnych potrzeb w ramach każdego zlecenia.

Wynikiem audytu zewnętrznego Kodu Źródłowego będzie raport zawierający zidentyfikowane niezgodności, problemy oraz rekomendacje i zalecenia.

Załącznik nr 4 do OPZ - Wymagania dotyczące testów.

WT-01 Wykonawca zobowiązany jest do przeprowadzenia testów jednostkowych na Środowisku Developerskim. Po zakończeniu testów Wykonawca zobowiązany jest do przedstawienia raportu z testów wraz z logiem z narzędzia, za pomocą którego były przeprowadzane testy, potwierdzającym wykonanie i liczbę poprawnie i błędnie przeprowadzonych testów.

WT-02 Wykonawca zobowiązany jest do wykonywania testów funkcjonalnych na Środowisku Testowym. Po zakończeniu testów Wykonawca jest zobowiązany do przedstawienia raportu z testów wraz ze scenariuszami testowymi oraz dowodów przeprowadzenia wyżej wymienionych testów. Dowodami mogą być zrzuty ekranu, wyciąg z logów Systemu, wyciąg z informacji z bazy danych Systemu.

WT-03 Wykonawca zobowiązany jest do przeprowadzenia testów wydajnościowych na Środowisku Testowym. Po zakończeniu testów Wykonawca zobowiązany jest do przedstawienia raportu z testów.

WT-04 Wykonawca zobowiązany jest do przeprowadzenia testów bezpieczeństwa na Środowisku Testowym. Po zakończeniu testów Wykonawca zobowiązany jest do przedstawienia raportu z testów.

WT-05 Wykonawca zobowiązany jest do opracowania mechanizmów automatycznych testów regresji wraz z narzędziami i procedurami ich uruchamiania i wykonywania.

WT-06 Wykonawca zobowiązany jest do skonfigurowania i uruchomienia narzędzia do wykonywania automatycznych testów regresji oraz zaimplementowania pierwszych scenariuszy wraz z pierwszą zgłoszoną Modyfikacją. Następnie Wykonawca będzie zobowiązany w ramach kolejnych zgłoszeń Modyfikacji do dodawania nowych scenariuszy dotyczących zaimplementowanych już funkcji Systemu.

WT-07 Zamawiający ma prawo rozszerzenia listy zagadnień testowych oraz zastrzega sobie prawo do zgłaszania zmian w proponowanych scenariuszach, które Wykonawca zobowiązany jest uwzględnić.

Załącznik nr 5 do OPZ - Poziom świadczenia usług (SLA).

Wykonawca zobowiązuje się świadczyć Przedmiot Umowy z zachowaniem następujących parametrów SLA (Service Level Agreement):

1. **Usługa Asysty Technicznej i Konserwacji:**

<table>
<tr><td>Kalendarz świadczenia usługi</td><td>Okno serwisowe w godzinach: 20.00 – 6.00.
Przyjmowanie i obsługa: Dni Robocze, w Godzinach Roboczych: 06:00 -18:00 z wyłączeniem awarii.</td></tr>
<tr><td>Czasy realizacji</td><td>
<table>
<tr><th>Lp.</th><th>Nazwa Wady</th><th>Czas Naprawy</th><th>Czas Obejścia</th></tr>
<tr><td>1.</td><td>Awaria</td><td>… (maksymalny Czas Naprawy 9 Godzin Roboczych, Czas Naprawy zostanie dostosowany do oferty Wykonawcy)</td><td>3 Godziny Robocze</td></tr>
<tr><td>2.</td><td>Błąd</td><td>…… (maksymalny Czas Naprawy 12 Godzin Roboczych, Czas Naprawy zostanie dostosowany do oferty Wykonawcy)</td><td>5 Godzin Roboczych</td></tr>
<tr><td>3.</td><td>Usterka</td><td>17 Godzin Roboczych</td><td>Nie dotyczy</td></tr>
<tr><td>4.</td><td>Pytania/Konsultacje</td><td>2 Dni Robocze lub w terminie uzgodnionym przez Strony</td><td>Nie dotyczy</td></tr>
<tr><td>5.</td><td>Pomyłka Użytkownika</td><td>9 Godzin Roboczych lub w terminie uzgodnionym przez Strony</td><td>Nie dotyczy</td></tr>
</table>
Definicje znajdują się w słowniku w rozdziale I Opisu Przedmiotu Zamówienia.
</td></tr>
</table>

Poziom dostępności usługi	**RPDS – rzeczywisty poziom dostępności Systemu dla Użytkowników** **RPDS ≥ 99 %** Miara poziomu świadczenia Usług Asysty Technicznej i Konserwacji (SLA) określona jako: RPDS = 100 * (GRM-CO-CN) /(GRM-CO) [%] gdzie: GRM – Liczba Godzin Roboczych w miesiącu CN – Łączny czas w Godzinach Roboczych Niedostępności Systemu w miesiącu. CO – Łączny czas w Godzinach Roboczych uzgodnionych z Zamawiającym Okien Serwisowych w miesiącu.
Lista i częstotliwość raportów	• Rzeczywisty poziom dostępności Systemu (RPDS) (miesięcznie).

2. Modyfikacja i Rozwój:

Kalendarz świadczenia Rozwoju	Przyjmowanie i obsługa: Dni Robocze w Godzinach Roboczych: 06:00-18:00		
Czasy realizacji	**Lp.**	**Nazwa**	**Czas realizacji**
	1.	Rozwój - Etap 1 (analiza wstępna)	10 dni kalendarzowych

	2.	Rozwój Etap 1 – (analiza pełna)	Ustalany w harmonogramie
	3.	Rozwój - Etap 2 (realizacja)	Ustalany w harmonogramie

Załącznik nr 6 do OPZ: Szczegółowe wymagania bezpieczeństwa w procesie utrzymania (ATiK) Systemu.

1. **Ramy odniesienia i zgodność**

1.1. Wykonawca zobowiązuje się, że proces utrzymania i rozwoju Systemu będzie realizowany w sposób zgodny z obowiązującymi standardami i regulacjami w zakresie bezpieczeństwa informacji i ochrony danych, w szczególności z:

a. **OWASP ASVS 5.0** – co najmniej na poziomie **Level 2** w obszarach: uwierzytelnianie, zarządzanie sesjami, zarządzanie danymi, logowanie, obsługa błędów i bezpieczeństwo API,
b. **OWASP Top 10** oraz **OWASP API Security Top 10**,
c. **Dyrektywą NIS2** oraz **ustawą o KSC** (**Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw Dz.U. 2026 poz. 252)** – w zakresie odporności, zapewnienia ciągłości działania, przygotowania i utrzymywania planów DRP/BCP oraz obowiązku raportowania incydentów do właściwych CSIRT,
d. **NIST Cybersecurity Framework** oraz normą **NIST SP 800-53** – w zakresie zarządzania bezpieczeństwem i kontrolami technicznymi,
e. **SANS/CWE Secure Coding Practices** – w zakresie stosowania wzorców bezpiecznego programowania i eliminacji typowych podatności,
f. **ISO/IEC 27001 i 27002** – w zakresie zarządzania bezpieczeństwem informacji oraz stosowania kontroli bezpieczeństwa,
g. **Rozporządzeniem KRI** – w zakresie minimalnych wymagań dla systemów teleinformatycznych,
h. **RODO** – w zakresie wdrożenia zasad **privacy by design** i **privacy by default** w całym cyklu życia systemu,
i. Rekomendacjami NASK i Cert Polska w zakresie cyberbezpieczeństwa w systemach publicznych

2. **SSDLC i bezpieczeństwo CI/CD**

2.1. Wykonawca jest zobowiązany do stosowania procesów Secure Software Development Lifecycle (SSDLC) obejmujących: planowanie, projektowanie (threat modeling), implementację (secure coding), weryfikację (testy bezpieczeństwa), wdrożenie (kontrola release), utrzymanie (monitoring i patching).

2.2. Systemy CI/CD muszą uwzględniać mechanizmy bezpieczeństwa, w tym:

a. automatyczne testy bezpieczeństwa (analiza statyczna, dynamiczna, analiza komponentów),
b. generowanie i utrzymywanie SBOM (Software Bill of Materials),
c. podpisywanie i weryfikację integralności artefaktów,
d. kontrolę zależności i wersji komponentów,
e. strategie bezprzerwowych wdrożeń (rolling updates, blue-green deployment lub równoważne).

3. Testy bezpieczeństwa i zarządzanie podatnościami

3.1. Wykonawca zobowiązuje się, że przed każdym wydaniem produkcyjnym oraz po każdej istotnej zmianie w kodzie źródłowym, architekturze lub konfiguracji Systemu przeprowadzi testy bezpieczeństwa obejmujące co najmniej:

analiza statyczna kodu źródłowego (SAST),

a. analiza dynamiczna (DAST),
b. analiza komponentów i bibliotek (SCA),
c. weryfikacja bezpieczeństwa API zgodnie z OWASP API Security Top 10,
d. aktualizacja SBOM.

3.2. Wykonawca zobowiązuje się, że wszystkie podatności zostaną zaklasyfikowane według metodologii CVSS 4.0 oraz usuwane w następujących terminach:

a. Critical (≥9.0) – eliminacja przed wdrożeniem,
b. High (7.0–8.9) – usunięcie do 7 dni roboczych,
c. Medium (4.0–6.9) – usunięcie do 30 dni roboczych,
d. Low (<4.0) – usunięcie w cyklu utrzymaniowym.

3.3. Wykonawca zobowiązuje się, że żaden release produkcyjny Systemu nie będzie zawierał podatności zaklasyfikowanych jako Critical lub High według CVSS 4.0.

3.4. Wykonawca zobowiązuje się do wdrożenia i utrzymywania w ramach świadczenia usług skutecznego procesu patch management, obejmującego**:**

a. monitorowanie podatności w komponentach, bibliotekach i środowisku,
b. szybką analizę wpływu,
c. przygotowanie i wdrożenie poprawek w wymaganych terminach,
d. przekazywanie Zamawiającemu raportów z działań naprawczych.

4. Zarządzanie komponentami i zależnościami

4.1. Wykonawca zobowiązuje się, że wszystkie wykorzystywane w Systemie komponenty, w tym frameworki, biblioteki, zależności, środowiska uruchomieniowe, systemy bazodanowe, kontenery oraz brokerzy wiadomości, będą utrzymywane w najnowszych stabilnych wersjach wspieranych przez producentów.

4.2. Wykonawca zobowiązuje się, że w ramach świadczenia usług nie będzie wykorzystywał komponentów:

a. EOL (End of Life),
b. niewspieranych przez producenta,
c. porzuconych lub znanych jako podatne na CVE.

4.3. Wykonawca zobowiązuje się do stałego monitorowania statusu wsparcia (EOL) wszystkich komponentów wykorzystywanych w

Systemie oraz do przygotowania i realizacji planów migracji przed zakończeniem okresu wsparcia producenta, w celu zapewnienia ciągłości i bezpieczeństwa działania Systemu.

5. Konfiguracja i hardening

5.1. Wykonawca zobowiązuje się, że wszystkie środowiska oraz serwery wykorzystywane do działania Systemu zostaną utwardzone zgodnie z uznanymi benchmarkami bezpieczeństwa (np. CIS lub równoważnymi), a w szczególności:

a. zostaną wyłączone wszystkie nieużywane usługi i porty,
b. zostanie zapewniona pełna separacja środowisk (produkcyjne, testowe, deweloperskie),
c. zostaną wdrożone mechanizmy ochrony przed atakami typu LFI (Local File Inclusion) i RFI (Remote File Inclusion),
d. zostanie zapewniona kontrola uprawnień i dostępów zgodnie z zasadą least privilege (minimalnych uprawnień).

6. Monitoring i wykrywanie incydentów

6.1. System musi zapewniać możliwość integracji z mechanizmami SIEM/SOAR w celu:

a. rejestrowania zdarzeń bezpieczeństwa,
b. korelacji logów,
c. reagowania na incydenty w czasie rzeczywistym.

6.2. Logi systemowe muszą być:

a. przechowywane w sposób uniemożliwiający ich modyfikację,
b. zawierać dane niezbędne do audytu (timestamp, użytkownik, adres IP, akcja).

6.3. Logi muszą być przechowywane zgodnie z polityką retencji, a minimalny okres przechowywania to 6 miesięcy, z możliwością przedłużenia do 2 lat w zależności od ryzyka, zgodności z RODO i polityką organizacji,

6.4. System musi umożliwiać automatyczne oznaczanie zdarzeń o znaczeniu RODO (np. dostęp do danych osobowych, ich eksport, edycja, usunięcie) oraz umożliwiać szybkie generowanie raportów z tych działań.

7. Ciągłość działania i odporność

2. Wykonawca zobowiązuje się, że System będzie, utrzymywany i rozwijany z wykorzystaniem mechanizmów zapewniających ciągłość działania i odporność, obejmujących w szczególności:

a. High Availability (HA) – zastosowanie rozwiązań gwarantujących wysoką dostępność usług i minimalizację przestojów,

b. Disaster Recovery (DR) – przygotowanie i utrzymywanie aktualnego planu odzyskiwania po awarii (DRP) oraz przeprowadzanie testów skuteczności tego planu nie rzadziej niż raz na 6 miesięcy,

c. Business Continuity Plan (BCP) – zapewnienie zgodności z wymaganiami dyrektywy NIS2 i ustawy o KSC w zakresie odporności, ciągłości działania i systemu zgłaszania incydentów.

8. Zarządzanie dostępem i hasłami

8.1. Wykonawca zobowiązuje się, że w ramach utrzymania i rozwoju Systemu zostanie wdrożona i egzekwowana polityka haseł zgodna z wytycznymi NIST SP 800-63B oraz ISO/IEC 27001, obejmująca co najmniej:

a. zakaz stosowania haseł znajdujących się w słownikach haseł kompromitowanych,

b. zapewnienie minimalnej długości i złożoności haseł stosowanych w Systemie,

c. wdrożenie mechanizmów wykrywania i blokowania haseł ujawnionych w znanych wyciekach danych,

d. regularne wymuszanie zmiany poświadczeń administracyjnych, zgodnie z najlepszymi praktykami bezpieczeństwa oraz wymaganiami Zamawiającego.

9. Raportowanie i kryteria akceptacji

9.1 Wykonawca zobowiązuje się, że po każdym wydaniu produkcyjnym Systemu przekaże Zamawiającemu komplet dokumentacji obejmującej:

a. raport z przeprowadzonych testów bezpieczeństwa (obejmujący SAST, DAST, SCA oraz testy bezpieczeństwa API),
b. zaktualizowany SBOM (Software Bill of Materials),
c. zestawienie wykrytych podatności wraz z ich klasyfikacją według metodologii CVSS 4.0,
d. potwierdzenie zgodności wszystkich komponentów z aktualnymi wymaganiami wsparcia producenta.

9.2 Wykonawca zobowiązuje się, że warunkiem przekazania Zamawiającemu release produkcyjnego jest spełnienie następujących kryteriów akceptacji:

a. brak podatności sklasyfikowanych jako Critical lub High według CVSS 4.0,
b. dostarczenie aktualnego i kompletnego SBOM,
c. przekazanie pozytywnie zweryfikowanych raportów bezpieczeństwa.

10. Odporność usługi

10.1 Wykonawca zobowiązuje się, że System będzie utrzymywany i rozwijany w sposób zapewniający jego odporność na zagrożenia bezpieczeństwa, ataki cybernetyczne oraz zakłócenia działania.

3. Odporność na ataki cybernetyczne musi być zapewniona poprzez:
   a. stosowanie zabezpieczeń zgodnych z OWASP ASVS 5.0 i OWASP Top 10 / API Security Top 10,
   b. identyfikację i mapowanie zagrożeń zgodnie z MITRE ATT&CK Framework oraz ich neutralizację poprzez odpowiednie mechanizmy obronne,
   c. projektowanie i wdrażanie architektury w oparciu o zasadę Zero Trust (NIST SP 800-207),
   d. wdrażanie benchmarków konfiguracji i hardeningu zgodnych z CIS Controls / CIS Benchmarks,
   e. stosowanie mechanizmów detekcji i reagowania zgodnie z NIST Cybersecurity Framework (Detect–Respond–Recover),
   f. monitorowanie i klasyfikację podatności zgodnie z CVSS 4.0,
   g. wdrażanie procedur zgodnych z ISO/IEC 27001, ISO/IEC 27035 (zarządzanie incydentami) oraz wymaganiami dyrektywy NIS2.

10.2 W ramach utrzymania Wykonawca zobowiązuje się do zapewnienia:

a. odporności na ataki sieciowe (DoS/DDoS, brute force, MITM) – poprzez stosowanie mechanizmów filtrowania, rate limiting i redundancję,
b. odporności na ataki aplikacyjne (SQLi, XSS, SSRF, RCE, CSRF, LFI/RFI) – poprzez kontrolę wejścia/wyjścia, walidację danych, bezpieczne sesje i sandboxing,
c. odporności na ataki na API – poprzez uwierzytelnianie, autoryzację, rate limiting, podpisywanie i szyfrowanie komunikacji,
d. odporności na ataki wektorowe w łańcuchu dostaw – poprzez kontrolę integralności kodu, SBOM, podpisywanie artefaktów i skanowanie komponentów,
e. odporności na ataki socjotechniczne i inżynierię społeczną – poprzez wdrażanie zabezpieczeń po stronie systemu (np. detekcja anomalii logowania, MFA) i mechanizmy edukacyjne dla użytkowników.

10.3 Wykonawca zobowiązuje się, że odporność usługi będzie systematycznie weryfikowana poprzez:

a. analizy zgodności z frameworkami bezpieczeństwa (OWASP, NIST, MITRE ATT&CK, CIS, ISO, NIS2) wykonywane:
   i. przed każdym release produkcyjnym zawierającym istotne zmiany funkcjonalne, architektoniczne lub infrastrukturalne,
   ii. w ramach procesu SSDLC – na etapie planowania (analiza wymagań bezpieczeństwa), projektowania (threat modeling),

weryfikacji (testy bezpieczeństwa) i wdrożenia (release readiness),

b. przeprowadzanie testów skuteczności wdrożonych mechanizmów ochronnych po każdej istotnej zmianie komponentów systemu, konfiguracji bezpieczeństwa lub infrastruktury,
c. przekazywanie Zamawiającemu raportów z analiz odporności wraz z rekomendacjami działań korygujących i terminami ich realizacji.

Załącznik nr 7 do OPZ: Wymagania funkcjonalne SOF2 konieczne dla przeprowadzenia konsolidacji ksiąg pomocniczych

1. Wprowadzenie

PFRON będzie wdrażał konsolidację ksiąg pomocniczych prowadzonych dotychczas w systemach SODIR, NEO i PWIND2. Po wdrożeniu konsolidacji system SOF2 stanie się jedynym miejscem prowadzenia rozrachunków z Kontrahentami PFRON oraz jedynym źródłem prawdy o tych rozrachunkach dla pozostałych systemów Funduszu. Systemy SODIR, NEO i PWIND2 przestają pełnić dotychczasową rolę rachunkowych ksiąg pomocniczych i przejdą do roli systemów dziedzinowych wypracowujących decyzje przekazywane do księgowania w SOF2.

Każdy rodzaj wypracowywanej przez systemy dziedzinowe PFRON decyzji będzie miał w SOF2 przypisany dedykowany schemat księgowy. Na podstawie przekazanej decyzji i jej metadanych SOF2 stworzy lub zaktualizuje rozrachunek z Kontrahentem, wygeneruje polecenia przelewów zgodnie z terminami płatności wynikającymi z rozrachunków, zaksięguje wyciągi bankowe oraz rozliczy wpłaty Kontrahentów zgodnie z decyzjami systemów dziedzinowych. Zapisy księgowe będą powstawać w miesiącu księgowym, w którym następuje rozksięgowanie, a rozrachunki będą przechowywać otrzymane z systemu dziedzinowego metadane, w szczególności okres pomocy, źródło finansowania czy też numer referencyjny programu pomocowego.

SOF2 udostępni poprzez API systemom dziedzinowym dostęp online do aktualnych sald rozrachunków, historii ich zmian, informacji o przelewach oraz danych Kontrahentów. Zmiany zachodzące po stronie SOF2 będą komunikowane do systemów dziedzinowych przez mechanizm powiadomień. Integracja będzie miała charakter dwukierunkowy i umożliwi systemom dziedzinowym prowadzenie postępowań administracyjnych oraz innych procesów decyzyjnych na podstawie bieżącego stanu rozrachunków.

Wymagania niniejszego załącznika mają charakter generyczny. Opisują mechanizmy, które muszą zostać wytworzone i wdrożone po stronie SOF2 niezależnie od konkretnego systemu dziedzinowego. Podłączenie poszczególnych systemów dziedzinowych do SOF2 według nowych zasad realizowane będzie w ramach odrębnych postępowań. W ramach niniejszego postępowania Wykonawca jest zobowiązany wytworzyć i wdrożyć mechanizmy generyczne opisane w niniejszym dokumencie. Weryfikacja prac nastąpi na obszarze gospodarki własnej PFRON obsługiwanym w SOF2 oraz integracji modułu MIDAS SOF2 z modułem FIX SOF2.

2. Zakres i granice

2.1. Zakres załącznika

Zakres zmian w systemie SOF2 objętych niniejszym załącznikiem obejmuje:

2.1.1. Rozbudowę rejestru Kontrahentów o wersjonowanie danych, mechanizm przyjmowania zmian od systemów dziedzinowych oraz udostępnianie danych Kontrahentów zwrotnie.

2.1.2. Rozbudowę planu kont o warstwę semantyczną wiążącą segmenty kont ze słownikami źródłowymi oraz mechanizm automatycznego zakładania kont analitycznych podczas rozksięgowania.

2.1.3. Wprowadzenie słownika rodzajów decyzji oraz mechanizmu definiowania schematów księgowych przypisanych do poszczególnych rodzajów decyzji.

2.1.4. Interfejs przyjmowania decyzji od systemów dziedzinowych wraz z walidacją, kolejkowaniem i rozksięgowywaniem.

2.1.5. Reguły i walidacje zmian na rozrachunkach obowiązujące niezależnie od źródła operacji.

2.1.6. Rozbudowę obsługi wyciągów bankowych i rozliczania wpłat zgodnie z decyzjami systemów dziedzinowych, w szczególności z uwzględnieniem zasad Ordynacji Podatkowej.

2.1.7. Udostępnianie danych online systemom dziedzinowym oraz mechanizm powiadomień o zmianach.

2.1.8. Usługę centralnego repozytorium kursów walut NBP dla systemów PFRON.

2.1.9. Audyt i logowanie operacji międzysystemowych z wykorzystaniem numeru decyzji jako identyfikatora korelacji.

2.2. Wyłączenia z zakresu

Poza zakresem niniejszego załącznika pozostają:

2.2.1. Wymagania niefunkcjonalne systemu SOF2 (wydajność, dostępność, bezpieczeństwo, skalowalność), objęte innymi częściami OPZ.

2.2.2. Mechanizmy wyceny i realizacji zleceń rozwoju systemu SOF2, objęte innymi częściami OPZ.

2.2.3. Podłączenie konkretnych systemów dziedzinowych (SODIR 3.0, NEO, PWIND2) do SOF2, realizowane w ramach odrębnych postępowań.

2.2.4. Wymagania na systemy dziedzinowe, stanowiące przedmiot postępowań dotyczących tych systemów.

2.3. Granica odpowiedzialności SOF2 oraz systemów dziedzinowych

W integracji SOF2 z systemami dziedzinowymi obowiązują następujące zasady podziału odpowiedzialności:

2.3.1. SOF2 będzie przechowywał i udostępniał dane na poziomie Kontrahenta PFRON. Analityka poniżej tego poziomu, w szczególności dane identyfikujące pracowników Beneficjenta oraz proporcje rozliczeń w rozbiciu na pracowników, pozostanie wyłącznie po stronie systemu dziedzinowego.

2.3.2. System dziedzinowy będzie wypracowywał decyzję wraz z kwotami rozbitymi na wartości słownikowe, w szczególności na pozycje słownika źródeł finansowania. SOF2 będzie przyjmował decyzję jako rozstrzygnięcie finalne i rozksięgowywał ją z zastosowaniem schematu księgowego przypisanego do jej rodzaju.

2.3.3. Źródłem prawdy o saldach rozrachunków Kontrahentów oraz historii tych rozrachunków będzie SOF2. Systemy dziedzinowe będą uzyskiwać dostęp do tych danych wyłącznie przez interfejsy udostępniane przez SOF2.

2.4. Walidacja poprzez wdrożenie

Mechanizmy wytworzone i wdrożone przez Wykonawcę w ramach niniejszego postępowania zostaną zweryfikowane na obszarze gospodarki własnej PFRON obsługiwanym w SOF2 oraz na integracji modułu MIDAS SOF2 z modułem FIX SOF2. Wskazane obszary będą pełnić rolę poligonu demonstracyjnego potwierdzającego poprawność i kompletność implementacji przed podłączeniem konkretnych systemów dziedzinowych do SOF2 w ramach odrębnych postępowań.

3. Pojęcia i definicje

Niniejsza sekcja definiuje pojęcia kluczowe dla zrozumienia wymagań zawartych w dokumencie. Definicje koncentrują się na terminach nowych lub na pojęciach, które w kontekście konsolidacji ksiąg pomocniczych zyskują nowe lub rozszerzone znaczenie w stosunku do dotychczasowej Dokumentacji Użytkownika modułu FIX SOF2 w innych przypadkach załącznik posługuje się definicjami zawartymi w powyższej dokumentacji.

Decyzja

Każde rozstrzygnięcie systemu dziedzinowego mające skutek finansowy, powodujące powstanie lub zmianę zobowiązania albo należności w rozrachunkach z Kontrahentem PFRON, konieczność aktualizacji zapisów księgowych albo utworzenie, modyfikację bądź anulowanie polecenia przelewu. Pojęcie szersze niż decyzja administracyjna w rozumieniu KPA. Nie każda formalna decyzja administracyjna jest przekazywana do SOF2, a do SOF2 trafiają również rozstrzygnięcia, które nie są formalnymi decyzjami administracyjnymi (np. automatyczne rozliczenie wpłaty).

Numer decyzji

Unikalny, niezmienny identyfikator decyzji w formacie KodSystemuDziedzinowego-NumerKolejny, nadawany po stronie systemu dziedzinowego. Jest czytelny dla człowieka i pełni równocześnie rolę identyfikatora korelacji umożliwiającego śledzenie operacji przez wszystkie etapy i komponenty (tracing).

Rodzaj decyzji

Typ decyzji określony w słowniku zarządzanym po stronie SOF2. Każdy rodzaj decyzji jest jednoznacznie powiązany z jednym schematem księgowym oraz określa wymagalność poszczególnych metadanych oraz ich krotność.

Schemat księgowy

Definicja sposobu rozksięgowania (dekretacji) decyzji danego rodzaju. Schemat wykorzystuje metadane decyzji do zbudowania numerów kont, określenia stron WN i MA, kwot, wyróżników transakcji i pozostałych elementów zapisów księgowowych.

Metadane decyzji
Zestaw atrybutów opisujących decyzję przekazywanych wraz z decyzją do SOF2 (m.in. numer decyzji, numer PFRON Kontrahenta, kwota, data wymagalności, rok i okres, rodzaj decyzji, opis, źródło finansowania, numer referencyjny programu pomocowego). Wymagalność poszczególnych metadanych jest zależna od rodzaju decyzji.

Kontrahent PFRON
podmiot gospodarczy identyfikowany w SOF2 przy użyciu unikalnego identyfikatora. Unikalny identyfikator jest obecny dla każdego Kontrahenta niezależnie od jego typu i stanowi podstawowy atrybut identyfikujący Kontrahenta w systemie. W przypadku Beneficjentów i Pracodawców Kontrahent jest dodatkowo identyfikowalny przy użyciu numeru PFRON, który pełni rolę identyfikatora biznesowego. Pojęcie obejmuje Beneficjentów (w terminologii SODIR, PWIND2) oraz Pracodawców (w terminologii NEO).

Źródło finansowania
słownik określający pochodzenie środków (m.in. środki własne PFRON, dotacja celowa MRPiPS). Wartość ze słownika będzie wykorzystywana w schematach księgowch do rozróżnienia kont księgowych.

System dziedzinowy
system zewnętrzny wobec SOF2, wypracowujący decyzje i przekazujący je do rozksięgowania. Po wdrożeniu konsolidacji w tej roli będą występowały m.in. SODIR 3.0, NEO, PWIND2.

Księga pomocnicza
Historyczny model integracji, w którym system dziedzinowy prowadził własną rachunkową księgę pomocniczą, a do SOF2 przekazywane były syntetyczne księgowania. Model będzie wygaszany w ramach projektów konsolidacji prowadzonych dla poszczególnych systemów dziedzinowych.

Gospodarka własna
Obszar działalności PFRON niezwiązany z realizacją zadań statutowych wobec Beneficjentów, obsługiwany w całości w ramach SOF2. W kontekście niniejszego dokumentu pełni rolę środowiska demonstracji poprawności wdrożenia mechanizmów generycznych.

4. Wymagania ogólne

Rozdział zawiera wymagania obowiązujące przekrojowo we wszystkich obszarach funkcjonalnych. Zapisanie ich w jednym miejscu pozwala uniknąć powielania tych samych reguł w wielu miejscach i zapewnić spójność ich stosowania.

WF-OG-01 Numer decyzji jako identyfikator korelacji
System SOF2 musi przyjmować, przechowywać i propagować numer decyzji otrzymany od systemu dziedzinowego jako identyfikator korelacji dla wszystkich operacji związanych z tą decyzją. Numer decyzji musi mieć format KodSystemuDziedzinowego-NumerKolejny i być czytelny dla człowieka. Nie dopuszcza się stosowania identyfikatorów technicznych typu UUID w roli numeru decyzji.

WF-OG-02 Walidacja unikalności numeru decyzji
Przy przyjęciu decyzji od systemu dziedzinowego SOF2 musi walidować unikalność numeru decyzji w skali całego systemu. Próba przekazania decyzji z numerem, który już istnieje w SOF2, musi być odrzucona, a do systemu dziedzinowego musi zostać zwrócona odpowiedź identyfikująca przyczynę odrzucenia.

WF-OG-03 Propagacja numeru decyzji
Numer decyzji musi być utrwalony w każdym artefakcie powstającym w wyniku przetwarzania decyzji, w szczególności w dokumencie księgowym, rozrachunku, poleceniu przelewu, zapisie w rejestrze zdarzeń oraz w treści powiadomienia wysyłanego do systemu dziedzinowego. Numer decyzji musi być dostępny jako kryterium wyszukiwania w każdym z tych miejsc.

WF-OG-04 Transakcyjność przetwarzania decyzji
Przetwarzanie pojedynczej decyzji po stronie SOF2 musi być transakcyjne w tym sensie, że jego wynikiem jest albo kompletne zaksięgowanie decyzji wraz z aktualizacją rozrachunku, utrwaleniem historii oraz wygenerowaniem powiadomień, albo oznaczenie decyzji jako błędnej bez częściowego zapisu skutków. Nie dopuszcza się stanu pośredniego, w którym decyzja jest częściowo rozksięgowana, rozrachunek jest częściowo zaktualizowany lub zapisy księgowe są niespójne z historią.

WF-OG-05 Historia zmian danych
Dla każdej jednostki danych przetwarzanych w obszarach opisanych w rozdziale 5 (w szczególności Kontrahenci, rozrachunki, dane decyzji, metadane schematów księgowych, słowniki) SOF2 musi prowadzić historię zmian. Historia musi zawierać co najmniej: moment dokonania zmiany, użytkownika lub system inicjujący zmianę, wartość przed zmianą, wartość po zmianie oraz numer decyzji będącej źródłem zmiany (jeżeli dotyczy).

WF-OG-06 Logowanie operacji międzysystemowych
SOF2 musi logować wszystkie operacje międzysystemowe (przyjęcie decyzji, udostępnienie danych, wysyłkę powiadomienia) z oznaczeniem precyzyjnego czasu i numeru decyzji jako kluczem korelacji. Zakres i retencja logu są doprecyzowane w obszarze AU (rozdział 5.5.2).

WF-OG-07 Integralność referencyjna metadanych
W każdym punkcie przetwarzania decyzji wartości metadanych o charakterze słownikowym (w szczególności rodzaj decyzji, źródło finansowania, program pomocowy, okres) muszą być walidowane pod kątem istnienia w odpowiednim słowniku. Decyzje zawierające nieznane wartości słownikowe muszą być odrzucane na etapie przyjęcia.

WF-OG-08 Zgodność z ograniczeniami analityki na poziomie Kontrahenta
SOF2 nie może przyjmować, przechowywać ani udostępniać danych analitycznych poniżej poziomu Kontrahenta PFRON, w szczególności danych identyfikujących pracowników Beneficjenta (PESEL, imię, nazwisko) oraz proporcji rozliczeń per pracownik. Takie dane, o ile pojawią się w komunikacji z systemami dziedzinowymi, muszą być odrzucone z metadanych decyzji przyjmowanej do rozksięgowania.

5. Wymagania funkcjonalne

Wymagania funkcjonalne zostały pogrupowane w pięć części logicznych odzwierciedlających rolę poszczególnych obszarów w całości rozwiązania. Kolejność odzwierciedla zależności: od fundamentów konfiguracyjnych, przez dynamikę przepływu decyzji, obsługę finansową, integrację zwrotną, po funkcje wspólne.

5.1. Część I - Konfiguracja i dane podstawowe

Część zawiera obszary definiujące fundament, który musi istnieć przed rozpoczęciem przetwarzania decyzji. Opisuje rejestr Kontrahentów, strukturę semantyczną planu kont, słownik rodzajów decyzji oraz definicje schematów księgowych.

5.1.1. Rejestr Kontrahentów (KR)

Rejestr Kontrahentów jest jednym z centralnych zasobów SOF2 i będzie centralnym miejscem przechowywania danych o podmiotach, z którymi PFRON prowadzi rozrachunki. Obszar opisuje rozbudowę rejestru o wersjonowanie, przyjmowanie zmian od systemów dziedzinowych oraz udostępnianie danych zwrotnie.

WF-KR-01 Wersjonowanie danych Kontrahenta

SOF2 musi przechowywać pełną historię zmian danych Kontrahenta z zachowaniem informacji o obowiązujących wartościach atrybutów w dowolnym momencie w przeszłości. Musi być możliwe odtworzenie stanu danych Kontrahenta na zadaną datę.

WF-KR-02 Przyjmowanie zmian danych Kontrahenta od systemów dziedzinowych

SOF2 musi udostępniać interfejs umożliwiający systemom dziedzinowym przekazywanie informacji o zmianach danych ewidencyjnych Kontrahenta. Wraz z informacją o zmianie musi być przekazana i zapisana informacja o czasie oraz sposobie pozyskania zmiany przez system dziedzinowy.

WF-KR-03 Akceptacja wybranych atrybutów przez Użytkownika Wewnętrznego

SOF2 musi umożliwiać oznaczenie wybranych atrybutów Kontrahenta jako wymagających akceptacji uprawnionego Użytkownika Wewnętrznego przed ich aktualizacją w rejestrze. Do momentu akceptacji zmiana jest widoczna jako oczekująca, a rejestr udostępnia nadal wartość sprzed zmiany. Lista atrybutów wymagających akceptacji musi być parametrem konfiguracyjnym systemu.

WF-KR-04 Udostępnianie danych Kontrahenta systemom dziedzinowym

SOF2 musi udostępniać systemom dziedzinowym interfejs odczytu aktualnych i historycznych danych Kontrahenta. Interfejs musi pozwalać na pobranie pełnego obrazu danych na zadaną datę oraz na pobranie dziennika zmian w zadanym przedziale czasowym.

WF-KR-05 Powiadomienie o zmianie danych Kontrahenta

Każda zmiana danych Kontrahenta (niezależnie od źródła) musi skutkować wysłaniem powiadomienia do zainteresowanych systemów dziedzinowych. Zasady subskrypcji i konfiguracji powiadomień opisane są w obszarze PW (rozdział 5.4.2).

5.1.2. Plan kont - semantyka segmentów (PK)

Obszar dotyczy rozbudowy istniejącego mechanizmu definicji segmentów konta o warstwę semantyczną. Warstwa semantyczna pozwala schematowi księgowemu na automatyczne zbudowanie numeru konta księgowego z metadanych decyzji.

WF-PK-01 Słownik źródłowy dla segmentu konta

SOF2 musi umożliwiać przypisanie każdemu segmentowi konta słownika źródłowego określającego dopuszczalne wartości tego segmentu. Słownikiem źródłowym może być zarówno słownik istniejący aktualnie w SOF2 (np. kontrahenci, źródła finansowania), jak i słownik wynikający z metadanych decyzji (np. rodzaj decyzji, program pomocowy).

WF-PK-02 Walidacja wartości segmentu przy budowie numeru konta

Przy budowie numeru konta w schemacie księgowym SOF2 musi walidować, że wartość podstawiana w segmencie istnieje w przypisanym do tego segmentu słowniku. Niezgodność musi skutkować odrzuceniem operacji rozksięgowania i zapisem błędu z numerem decyzji jako kluczem.

WF-PK-03 Reguła mapowania metadanych na segmenty konta

SOF2 musi umożliwiać definicję reguły mapowania wskazującej, które metadane decyzji są podstawiane w których segmentach konta. Reguła jest elementem schematu księgowego przypisanego do rodzaju decyzji (obszar SK).

WF-PK-04 Zarządzanie słownikami źródłowymi

SOF2 musi umożliwiać uprawnionemu Użytkownikowi Wewnętrznemu zarządzanie słownikami źródłowymi wykorzystywanymi w segmentach planu kont, w tym dodawanie, oznaczanie jako nieaktywne oraz wersjonowanie pozycji słownikowych. Historia zmian słowników jest prowadzona zgodnie z wymaganiem WF-OG-05.

WF-PK-05 Prezentacja semantyczna numeru konta

SOF2 musi prezentować numer konta w widokach operacyjnych i raportach w sposób umożliwiający odczyt wartości każdego segmentu wraz z jego znaczeniem słownikowym. Sposób prezentacji musi być konfigurowalny i uwzględniać potrzeby różnych typów użytkowników.

5.1.3. Słownik rodzajów decyzji i metadanych (SD)

Obszar opisuje zarządzanie centralnym słownikiem rodzajów decyzji przyjmowanych od systemów dziedzinowych. Każdy rodzaj decyzji w tym słowniku jest punktem zbieżności pomiędzy metadanymi wysyłanymi przez system dziedzinowy a schematem księgowym stosowanym po stronie SOF2.

WF-SD-01 Definiowanie rodzajów decyzji

SOF2 musi umożliwiać uprawnionemu Użytkownikowi Wewnętrznemu definiowanie rodzajów decyzji przyjmowanych od systemów dziedzinowych. Dla każdego rodzaju decyzji słownik musi przechowywać co najmniej: kod, nazwę, opis, identyfikator systemu dziedzinowego źródłowego dla tego rodzaju, stan (aktywny, wygaszany, nieaktywny).

WF-SD-02 Powiązanie rodzaju decyzji ze schematem księgowym
Każdy rodzaj decyzji musi być powiązany z dokładnie jednym schematem księgowym aktualnym w danym momencie. Nie dopuszcza się istnienia aktywnego rodzaju decyzji bez przypisanego schematu.

WF-SD-03 Definicja wymagalności metadanych
Dla każdego rodzaju decyzji słownik musi przechowywać definicję wymagalności poszczególnych metadanych (wymagane, opcjonalne, niedopuszczalne). Definicja wymagalności jest wykorzystywana przy walidacji decyzji na etapie przyjęcia (obszar PD).

WF-SD-04 Wersjonowanie słownika rodzajów decyzji
Słownik rodzajów decyzji musi być wersjonowany w sposób umożliwiający jednoczesne obsługiwanie decyzji zgodnych z różnymi wersjami słownika (np. decyzji przyjętych przed i po zmianie definicji wymagalności metadanych). Każda decyzja musi być trwale powiązana z wersją słownika obowiązującą w momencie jej przyjęcia.

WF-SD-05 Publikacja słownika dla systemów dziedzinowych
SOF2 musi udostępniać systemom dziedzinowym interfejs odczytu aktualnej i historycznych wersji słownika rodzajów decyzji. Interfejs musi zawierać informację o wymagalności metadanych oraz o stanie poszczególnych pozycji słownika.

5.1.4. Schematy księgowe dla decyzji dziedzinowych (SK)
Obszar opisuje mechanizm definiowania schematów księgowych wykorzystywanych do rozksięgowywania decyzji przekazanych z systemów dziedzinowych. Obecny w SOF2 mechanizm „scenariuszy księgowania dokumentów" stanowi punkt wyjścia dla rozbudowy opisanej poniżej i będzie wykorzystywany również przez moduł MIDAS SOF2.

WF-SK-01 Definiowanie schematu księgowego
SOF2 musi umożliwiać uprawnionemu Użytkownikowi Wewnętrznemu definiowanie schematu księgowego jako sekwencji zapisów księgowych, w której każdy zapis określa stronę (WN, MA), regułę budowy numeru konta (odwołującą się do segmentów planu kont i metadanych decyzji zgodnie z wymaganiami obszaru PK), regułę wyznaczenia kwoty oraz regułę przypisania do transakcji rozrachunkowej.

WF-SK-02 Walidacja kompletności schematu
Przed zapisem schematu księgowego SOF2 musi walidować jego kompletność i spójność, w szczególności: bilansowanie stron WN i MA dla typowych przypadków, istnienie wszystkich odwoływanych segmentów i słowników, kompletność reguł budowy numerów kont, kompletność reguł wyznaczania transakcji rozrachunkowej.

WF-SK-03 Symulacja schematu na przykładowej decyzji
SOF2 musi umożliwiać uprawnionemu Użytkownikowi Wewnętrznemu przeprowadzenie symulacji schematu księgowego na przykładowej decyzji (bez faktycznego księgowania). Wynikiem symulacji musi być pełny podgląd zapisów księgowych, jakie powstałyby po rozksięgowaniu, wraz z komunikatami o ewentualnych problemach.

WF-SK-04 Wersjonowanie schematów księgowych
Schematy księgowe muszą być wersjonowane zgodnie z zasadami obowiązującymi dla słownika rodzajów decyzji (WF-SD-04). Decyzja przyjęta w momencie obowiązywania określonej wersji schematu musi być rozksięgowana z użyciem tej wersji tj. nowa wersja schematu księgowego musi mieć atrybut określający od jakiego momentu obowiązuje z ustawienie momentu zatwierdzenia jako czasu obowiązywania „od".

WF-SK-05 Rozbudowa mechanizmu scenariuszy księgowania dokumentów
Istniejący w SOF2 mechanizm scenariuszy księgowania dokumentów musi zostać rozbudowany tak, aby spełniał wszystkie wymagania opisane w niniejszym obszarze, w szczególności w zakresie wiązania z rodzajem decyzji, wersjonowania oraz wykorzystania semantyki segmentów planu kont. Rozbudowa musi zachować wsteczną zgodność z istniejącymi scenariuszami księgowania dokumentów wykorzystywanymi przez moduł MIDAS i inne ewidencje pomocnicze.

WF-SK-06 Obsługa decyzji korygujących i stornujących
Decyzje korygujące i stornujące muszą być obsługiwane jako rodzaje decyzji z własnym schematem księgowym, na zasadach identycznych jak pozostałe decyzje. Nie dopuszcza się specjalnego traktowania takich decyzji poza mechanizmem schematów księgowych.

5.2. Cześć II - Przepływ decyzji

Część opisuje dynamikę przetwarzania decyzji: od przyjęcia od systemu dziedzinowego, przez walidację i rozksięgowanie, po aktualizację rozrachunków. Zawiera również reguły zmian na rozrachunkach, które wykraczają poza pojedynczą decyzję i dotyczą wszystkich rozrachunków niezależnie od źródła.

5.2.1. Przyjmowanie decyzji od systemów dziedzinowych (PD)

Obszar opisuje interfejs przyjmowania decyzji z systemów dziedzinowych oraz reguły postępowania z decyzją od momentu wywołania interfejsu do momentu przekazania jej do rozksięgowania.

WF-PD-01 Interfejs przyjmowania decyzji
SOF2 musi udostępniać systemom dziedzinowym interfejs API umożliwiający przekazanie decyzji wraz z kompletem metadanych wymaganych dla jej rodzaju. Interfejs musi być zgodny z formatem wymiany danych uzgodnionym w fazie analizy przedwdrożeniowej.

WF-PD-02 Kolejkowanie przyjętych decyzji
Każda decyzja przyjęta przez interfejs musi być zakolejkowana w SOF2 wraz z oznaczeniem precyzyjnego czasu przyjęcia. Kolejność przetwarzania decyzji musi odpowiadać kolejności ich przyjęcia, o ile nie występują pomiędzy nimi zależności funkcjonalne wymuszające inną kolejność.

WF-PD-03 Walidacja syntaktyczna i semantyczna
Przed zakolejkowaniem decyzji SOF2 musi wykonać walidację zawierającą co najmniej: poprawność formatu numeru decyzji, unikalność numeru decyzji (WF-OG-02), istnienie Kontrahenta w rejestrze, istnienie rodzaju decyzji w słowniku, kompletność metadanych

zgodnie z definicją wymagalności (WF-SD-03), integralność referencyjną wartości słownikowych (WF-OG-07).

WF-PD-04 Odrzucenie decyzji z przyczyną
Decyzja, która nie przeszła walidacji, musi być odrzucona z jednoczesnym zwróceniem do systemu dziedzinowego informacji o przyczynie odrzucenia. Informacja musi być jednoznaczna i umożliwiać systemowi dziedzinowemu skuteczną diagnozę i ponowne przesłanie po skorygowaniu.

WF-PD-05 Potwierdzenie przyjęcia decyzji
Po pomyślnej walidacji i zakolejkowaniu decyzji SOF2 musi zwrócić do systemu dziedzinowego potwierdzenie przyjęcia zawierające numer decyzji oraz precyzyjny czas przyjęcia. Potwierdzenie musi być zwracane synchronicznie w ramach wywołania interfejsu.

WF-PD-06 Obsługa ponownego przesłania
Przesłanie decyzji z numerem już istniejącym w SOF2 musi skutkować odpowiedzią identyfikującą decyzję jako już przyjętą wraz ze zwrotem statusu jej przetwarzania. Operacja musi być obsługiwana poprzez odrzucenie duplikatu zgodnie WF-OG-02.

WF-PD-07 Rozksięgowanie po przyjęciu
Przyjęta i zwalidowana decyzja musi być przekazana do rozksięgowania zgodnie z obszarem KD (rozdział 5.2.2). Oznaczenie decyzji jako rozksięgowanej lub błędnej po rozksięgowaniu musi być dostępne dla systemu dziedzinowego poprzez interfejs odczytu statusu.

5.2.2. Rozksięgowanie decyzji i aktualizacja rozrachunków (KD)
Obszar opisuje, co dzieje się z decyzją po przyjęciu: zastosowanie schematu księgowego, utworzenie dokumentu księgowego, utworzenie lub aktualizację rozrachunku.

WF-KD-01 Zastosowanie schematu księgowego
Dla każdej przyjętej decyzji SOF2 musi zastosować schemat księgowy przypisany do jej rodzaju w wersji obowiązującej w momencie przyjęcia decyzji (WF-SK-04). Wynikiem zastosowania schematu jest dokument księgowy zawierający komplet zapisów WN i MA zgodnych z zasadą dwustronności zapisów księgowych.

WF-KD-02 Utworzenie lub aktualizacja rozrachunku
Rozksięgowanie decyzji musi skutkować utworzeniem lub aktualizacją rozrachunku z Kontrahentem, zgodnie z logiką rodzaju decyzji i schematu księgowego. Rozrachunek musi zawierać numer decyzji jako atrybut umożliwiający jego odnalezienie.

WF-KD-03 Zapis metadanych decyzji w rozrachunku
Rozrachunek powstały lub zaktualizowany na skutek decyzji musi przechowywać metadane decyzji niezbędne do późniejszej identyfikacji i analizy, w szczególności rok i okres, którego dotyczy decyzja, źródło finansowania, numer referencyjny programu pomocowego, rodzaj decyzji, numer decyzji oraz skrócony opis decyzji.

WF-KD-04 Powiązanie decyzja-dokument-rozrachunek
SOF2 musi trwale przechowywać powiązanie pomiędzy decyzją, dokumentem księgowym powstałym w wyniku jej rozksięgowania oraz rozrachunkiem powstałym lub

zaktualizowanym w wyniku tego rozksięgowania. Powiązanie musi być dostępne dwukierunkowo, z decyzji do rozrachunku oraz z rozrachunku do decyzji.

WF-KD-05 Okres księgowy rozksięgowania
Zapisy księgowe wynikające z decyzji muszą być księgowane w miesiącu księgowym, w którym powstaje operacja rozksięgowania, niezależnie od roku i okresu pomocy, którego decyzja dotyczy. Rok i okres pomocy są przechowywane jako metadane rozrachunku (WF-KD-03), a nie jako data księgowania.

WF-KD-06 Obsługa błędu rozksięgowania
Błąd na etapie rozksięgowania, na przykład problem z walidacją segmentu konta zgodnie z WF-PK-02 lub brak wymaganego konta syntetycznego zgodnie z WF-PK-07, musi skutkować oznaczeniem decyzji jako błędnej, zapisem przyczyny błędu w logu z numerem decyzji jako kluczem oraz wysłaniem powiadomienia do systemu dziedzinowego. Decyzja błędna nie modyfikuje rozrachunków Kontrahenta do czasu ponownego skutecznego rozksięgowania.

5.2.3. Reguły i walidacje zmian na rozrachunkach (ZR)
Obszar zbiera reguły walidacji obowiązujące przy każdej zmianie na rozrachunku, niezależnie od tego, czy zmiana wynika z decyzji systemu dziedzinowego, operacji automatycznej w SOF2, czy interwencji Użytkownika Wewnętrznego.

WF-ZR-01 Ograniczenie zmian przed terminem płatności
SOF2 musi zapewnić konfigurowalny parametr określający najpóźniejszy moment, w którym dopuszczalna jest zmiana rozrachunku skutkująca modyfikacją zaplanowanej płatności. Wartość domyślna parametru to koniec dnia poprzedzającego termin płatności danego rozrachunku. Po upłynięciu tego momentu zmiany na rozrachunku są blokowane.

WF-ZR-02 Zabezpieczenie wygenerowanych paczek przelewów
Jeżeli rozrachunek został objęty wygenerowaną paczką przelewów, zmiany skutkujące modyfikacją kwoty, terminu lub stanu płatności muszą być odrzucane niezależnie od wartości parametru z WF-ZR-01. Decyzja usiłująca wprowadzić taką zmianę musi być odrzucona z jednoznaczną przyczyną, a system dziedzinowy musi mieć możliwość rozpoznania tego przypadku.

WF-ZR-03 Dopuszczalne typy zmian w zależności od stanu rozrachunku
SOF2 musi utrzymywać macierz dopuszczalnych typów zmian w zależności od stanu rozrachunku, na przykład otwarty, częściowo rozliczony, w trakcie windykacji, zamknięty. Macierz musi być konfigurowalna przez uprawnionego Użytkownika Wewnętrznego. Próba zmiany niezgodnej z macierzą musi być odrzucona.

WF-ZR-04 Walidacje terminów płatności w decyzjach o zmianę
Decyzje wprowadzające zmianę terminu płatności muszą przechodzić walidację, że nowy termin dotyczy wyłącznie przyszłości względem daty operacji. Walidacja po stronie SOF2 jest obowiązkowa niezależnie od ewentualnej walidacji po stronie systemu dziedzinowego.

WF-ZR-05 Komunikowanie odrzucenia zmiany do systemu dziedzinowego
Każde odrzucenie zmiany na rozrachunku wynikającej z decyzji systemu dziedzinowego musi być zakomunikowane do systemu dziedzinowego z jednoznacznym kodem i opisem

przyczyny. Komunikacja musi umożliwiać systemowi dziedzinowemu podjęcie odpowiedniej akcji, w tym wypracowanie decyzji kompensującej.

5.3. Cześć III - Operacje rozrachunkowe i płatności

Część opisuje operacje wykonywane przez SOF2 z rozrachunkami oraz związanymi z nimi płatnościami: generowanie poleceń przelewu, obsługę wyciągów bankowych, rozliczanie wpłat

5.3.1. Generowanie poleceń przelewu (GP)

Obszar opisuje mechanizm tworzenia poleceń przelewu na podstawie zobowiązań w rozrachunkach oraz ich zaawansowanie przez cykl życia (przygotowane, wysłane, wykonane).

WF-GP-01 Generowanie poleceń przelewu z zobowiązań

SOF2 musi automatycznie generować polecenia przelewu na podstawie zobowiązań zapisanych w rozrachunkach z Kontrahentami, uwzględniając terminy płatności określone w tych rozrachunkach. Polecenie przelewu musi zawierać numer decyzji jako element pozwalający na retrospekcję.

WF-GP-02 Paczkowanie przelewów

SOF2 musi umożliwiać łączenie poleceń przelewu w paczki przelewów zgodnie z regułami konfigurowanymi przez uprawnionego Użytkownika Wewnętrznego. Wygenerowanie paczki wymusza ochronę obejmowanych nią rozrachunków zgodnie z WF-ZR-02.

WF-GP-03 Integracja z modułem Elektronicznych Wyciągów Bankowych

SOF2 musi wykorzystywać istniejący moduł EWB do emisji elektronicznych plików przelewów zgodnych z wymaganiami banku obsługującego rachunek. Propagacja numeru decyzji do pliku przelewu musi być zachowana w zakresie, w jakim pozwala na to format pliku banku.

WF-GP-04 Status polecenia przelewu

SOF2 musi przechowywać i udostępniać status polecenia przelewu obejmujący co najmniej stany przygotowane, przekazane do banku, potwierdzone przez bank do wykonania, wykonane po zaksięgowaniu wyciągu bankowego, odrzucone przez bank, wycofane.

WF-GP-05 Udostępnianie statusu przelewu systemom dziedzinowym

Status polecenia przelewu musi być dostępny dla systemu dziedzinowego poprzez interfejs opisany w obszarze UD (rozdział 5.4.1) oraz być przedmiotem powiadomień opisanych w obszarze PW (rozdział 5.4.2). W szczególności system dziedzinowy musi otrzymywać informację o potwierdzeniu przyjęcia dyspozycji przez bank jeszcze przed zaksięgowaniem wyciągu.

5.3.2. Obsługa wyciągów bankowych i kojarzenie wpłat (WB)

Obszar stanowi rozbudowę istniejącej obsługi wyciągów bankowych w FIX o nowe elementy wynikające z integracji z systemami dziedzinowymi.

WF-WB-01 Import i księgowanie wyciągów bankowych
SOF2 musi zachować istniejącą funkcjonalność importu i księgowania wyciągów bankowych z rozszerzeniami opisanymi w dalszych wymaganiach niniejszego obszaru.

WF-WB-02 Identyfikacja Kontrahenta w pozycji wyciągu
Dla każdej pozycji wyciągu dotyczącej wpłaty SOF2 musi automatycznie identyfikować Kontrahenta na podstawie danych z wyciągu bankowego. Reguły identyfikacji muszą być konfigurowalne i uwzględniać co najmniej numer PFRON, NIP lub REGON w treści przelewu oraz identyfikator rachunku bankowego Kontrahenta zapisany w rejestrze.

WF-WB-03 Obsługa wpłat nierozpoznanych
Wpłata, dla której nie udało się jednoznacznie zidentyfikować Kontrahenta, musi być zarejestrowana jako wpłata nierozpoznana w dedykowanym obszarze wymagającym interwencji Użytkownika Wewnętrznego. Proces identyfikacji i przypisania wpłaty musi być wspierany narzędziami wyszukiwania oraz podpowiedzi.

WF-WB-04 Przekazanie wpłaty do systemu dziedzinowego celem wypracowania decyzji o rozliczeniu
Po zidentyfikowaniu Kontrahenta SOF2 musi przekazać informację o wpłacie do właściwego systemu dziedzinowego celem wypracowania decyzji o jej rozliczeniu zgodnie z obszarem RW (rozdział 5.3.3). Kryteria kierowania wpłaty do konkretnego systemu dziedzinowego muszą być konfigurowalne.

WF-WB-05 Stan wpłaty przed otrzymaniem decyzji o rozliczeniu
Do momentu otrzymania decyzji systemu dziedzinowego o rozliczeniu wpłaty SOF2 musi przechowywać wpłatę jako nierozliczoną na dedykowanym koncie, na przykład koncie wpłat do wyjaśnienia, z zachowaniem powiązania z Kontrahentem.

5.3.3. Rozliczanie wpłat wg decyzji systemu dziedzinowego (RW)
Obszar opisuje, jak SOF2 rozlicza wpłatę Kontrahenta na konkretne rozrachunki zgodnie z decyzją wypracowaną przez system dziedzinowy.

WF-RW-01 Przyjęcie decyzji o rozliczeniu wpłaty
SOF2 musi przyjmować decyzje systemu dziedzinowego o sposobie rozliczenia konkretnej wpłaty na konkretne rozrachunki Kontrahenta. Decyzja jest przekazywana przez interfejs opisany w obszarze PD (rozdział 5.2.1) i rozksięgowywana zgodnie z obszarem KD (rozdział 5.2.2).

WF-RW-02 Realizacja rozliczenia zgodnie z Ordynacją podatkową
Schemat księgowy stosowany do rozksięgowania decyzji o rozliczeniu wpłaty musi realizować podział wpłaty na pokrycie kwoty głównej i odsetek zgodnie z przekazaną decyzją. System dziedzinowy jest odpowiedzialny za wypracowanie decyzji zgodnej z zasadami Ordynacji Podatkowej. SOF2 rozlicza wpłatę wg kwot określonych w decyzji.

WF-RW-03 Rozliczenie w podziale na źródła finansowania
Jeżeli decyzja o rozliczeniu wpłaty zawiera kwoty rozbite na pozycje słownika źródeł finansowania, SOF2 musi rozliczyć wpłatę zgodnie z tym podziałem, prowadząc osobne zapisy księgowe dla każdego źródła. Dekompozycja na poziomy niższe niż źródło

finansowania, na przykład per pracownik, pozostaje poza zakresem SOF2 zgodnie z WF-OG-08.

WF-RW-04 Aktualizacja sald rozrachunków
Po rozksięgowaniu decyzji o rozliczeniu wpłaty SOF2 musi zaktualizować salda objętych rozrachunków oraz zamknąć rozrachunki w pełni rozliczone. Zmiana stanu rozrachunku jest przedmiotem powiadomienia do systemu dziedzinowego zgodnie z obszarem PW.

WF-RW-05 Obsługa wpłaty niepasującej do żadnego rozrachunku
Jeżeli system dziedzinowy nie wypracuje decyzji o rozliczeniu wpłaty w wyznaczonym czasie lub decyzja wskazuje, że wpłata nie może być rozliczona z istniejącymi rozrachunkami, SOF2 musi utrzymywać wpłatę jako nadpłatę Kontrahenta, oczekującą na kolejne decyzje dyspozycyjne.

5.4. Cześć IV - Udostępnianie danych i powiadomienia

Część opisuje integrację zwrotną: dane, które SOF2 udostępnia systemom dziedzinowym oraz mechanizm powiadomień o zmianach. Bez tej części systemy dziedzinowe nie mogłyby skutecznie wypracowywać kolejnych decyzji, ponieważ musiałyby działać w oderwaniu od aktualnego stanu rozrachunków.

5.4.1. Udostępnianie danych online systemom dziedzinowym (UD)

Obszar opisuje zakres i formę danych, które SOF2 udostępnia do odczytu systemom dziedzinowym.

WF-UD-01 Odczyt aktualnych sald rozrachunków Kontrahenta
SOF2 musi udostępniać interfejs odczytu aktualnych sald rozrachunków dla wskazanego Kontrahenta, obejmujący wszystkie otwarte rozrachunki z podziałem na kwotę główną, odsetki, saldo oraz stan. Każda pozycja musi zawierać numer decyzji, z której wynika oraz pozostałe metadane zgodnie z WF-KD-03.

WF-UD-02 Odczyt historii zmian rozrachunków
SOF2 musi udostępniać interfejs odczytu historii zmian rozrachunków wskazanego Kontrahenta w zadanym przedziale czasowym. Historia musi zawierać wszystkie zmiany z oznaczeniem momentu zmiany, numeru decyzji będącej źródłem zmiany oraz wartości przed i po zmianie.

WF-UD-03 Odczyt informacji o przelewach Kontrahenta
SOF2 musi udostępniać interfejs odczytu informacji o poleceniach przelewu dotyczących wskazanego Kontrahenta, obejmujący zarówno przelewy zlecone przez PFRON na rzecz Kontrahenta, jak i wpłaty otrzymane od Kontrahenta. Każda pozycja musi zawierać status zgodnie z WF-GP-04, powiązanie z rozrachunkami oraz odpowiednie numery decyzji.

WF-UD-04 Raportowy przegląd po stronie SOF2
Dane udostępniane systemom dziedzinowym musi być również dostępne w formie raportowej po stronie SOF2 dla uprawnionych Użytkowników Wewnętrznych, z możliwością wydruku i eksportu. Zakres informacji prezentowanych w raporcie musi pokrywać co najmniej zakres dostępny przez interfejsy opisane w WF-UD-01, WF-UD-02 i WF-UD-03.

WF-UD-05 Spójność danych online
Dane udostępniane przez interfejsy opisane w niniejszym obszarze muszą odzwierciedlać aktualny stan księgowy SOF2 w czasie zbliżonym do rzeczywistego. Dopuszczalne opóźnienie pomiędzy operacją księgową a widocznością jej skutku przez interfejs odczytu musi być mierzalne i zgodne z uzgodnieniami poziomu świadczenia usługi.

5.4.2. Powiadomienia push (PW)
Obszar opisuje mechanizm aktywnego powiadamiania systemów dziedzinowych o zmianach po stronie SOF2. Mechanizm uzupełnia interfejsy odczytu z obszaru UD, umożliwiając systemom dziedzinowym reagowanie na zmiany bez konieczności cyklicznego odpytywania SOF2.

WF-PW-01 Wysyłka powiadomień o zmianach sald rozrachunków
SOF2 musi wysyłać do zainteresowanych systemów dziedzinowych powiadomienia o każdej zmianie salda rozrachunku Kontrahenta. Powiadomienie musi zawierać co najmniej numer PFRON Kontrahenta, identyfikator rozrachunku, numer decyzji będącej źródłem zmiany oraz wartości salda przed i po zmianie.

WF-PW-02 Wysyłka powiadomień o statusach przelewów
SOF2 musi wysyłać do zainteresowanych systemów dziedzinowych powiadomienia o każdej zmianie statusu polecenia przelewu zgodnie z WF-GP-04. Powiadomienie musi być wysłane bezzwłocznie, w szczególności w momencie potwierdzenia przyjęcia dyspozycji przez bank i niezależnie od późniejszego księgowania wyciągu bankowego.

WF-PW-03 Wysyłka powiadomień o zmianach danych Kontrahenta
SOF2 musi wysyłać do zainteresowanych systemów dziedzinowych powiadomienia o każdej zmianie danych Kontrahenta w rejestrze zgodnie z obszarem KR. Zasady dotyczą zarówno zmian wprowadzonych przez sam SOF2, jak i zmian przyjętych od innych systemów dziedzinowych.

WF-PW-04 Subskrypcja powiadomień
SOF2 musi umożliwiać konfigurację, który system dziedzinowy otrzymuje jakie rodzaje powiadomień i dla jakich zakresów danych. Konfiguracja musi być zarządzana przez uprawnionego Użytkownika Wewnętrznego i uwzględniać zarówno reguły domyślne, jak i wyjątki dla konkretnych systemów.

WF-PW-05 Gwarancja dostarczenia powiadomień
Mechanizm powiadomień musi zapewniać dostarczenie powiadomienia do systemu dziedzinowego, z obsługą ponownych prób w razie niedostępności odbiorcy. Historia wysyłki i potwierdzeń odbioru musi być dostępna dla analizy zgodnie z obszarem AU.

WF-PW-06 Propagacja numeru decyzji w powiadomieniu
Każde powiadomienie, którego przyczyną jest decyzja systemu dziedzinowego, musi zawierać numer decyzji jako element umożliwiający odbiorcy powiązanie powiadomienia ze swoim procesem. Numer decyzji jest nośnikiem korelacji zgodnie z WF-OG-01.

5.5. Cześć V – Funkcje wspólne

Część zawiera wymagania, które mają charakter usługowy dla całej organizacji (kursy walut NBP) albo przekrojowy wobec wszystkich procesów (audyt).

5.5.1. Usługa kursów walut NBP (KW)

Obszar odpowiedzialny za rolę SOF2 jako centralnego repozytorium kursów walut obcych dla systemów PFRON

WF-KW-01 Automatyczne pobieranie kursów walut z NBP

SOF2 musi automatycznie pobierać średnie kursy walut obcych (w szczególności EUR/PLN) z publicznego Web API Narodowego Banku Polskiego. Pobieranie musi obejmować tabele kursów typu A (kursy średnie głównych walut obcych).

WF-KW-02 Harmonogram pobierania

SOF2 musi pobierać kursy walut automatycznie w trybie cyklicznym, co najmniej raz dziennie w dni robocze, po godzinie publikacji tabeli przez NBP. Harmonogram musi być konfigurowalny przez uprawnionego Użytkownika Wewnętrznego.

WF-KW-03 Przechowywanie kursów historycznych

SOF2 musi przechowywać wszystkie pobrane kursy walut z zachowaniem daty obowiązywania oraz numeru tabeli NBP. Dane historyczne muszą być dostępne do odczytu bez ograniczeń czasowych.

WF-KW-04 Udostępnianie kursów systemom PFRON

SOF2 musi udostępniać interfejs odczytu kursów walut dla pozostałych systemów PFRON, w szczególności dla SODIR 3.0 na potrzeby przeliczania wartości pomocy publicznej i pomocy de minimis na euro zgodnie z art. 11 ust. 3 ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej.

WF-KW-05 Obsługa braku kursu

Dla zapytań dotyczących dni, w których NBP nie publikuje tabeli (weekendy, święta), SOF2 musi zwracać odpowiedź identyfikującą brak kursu na wskazany dzień. Zasady stosowania kursu z poprzedniego dnia roboczego leżą po stronie systemu odpytującego.

WF-KW-06 Monitorowanie dostępności źródła

SOF2 musi monitorować skuteczność pobierania kursów i w przypadku niepowodzenia (np. niedostępność API NBP) powiadomić uprawnionego Użytkownika Wewnętrznego. Niepobrane kursy muszą być pobrane przy następnej możliwości.

5.5.2. Audyt i logowanie operacji międzysystemowych (AU)

Obszar opisuje rejestr zdarzeń prowadzony przez SOF2 na potrzeby audytu, analizy błędów i retrospekcji łańcuchów operacji międzysystemowych.

WF-AU-01 Rejestr zdarzeń operacji międzysystemowych

SOF2 musi prowadzić rejestr zdarzeń obejmujący wszystkie operacje międzysystemowe, w szczególności: przyjęcie decyzji od systemu dziedzinowego, wywołanie interfejsu odczytu danych, wysłanie powiadomienia, odbiór potwierdzenia dostarczenia powiadomienia, błąd

przetwarzania decyzji. Każdy zapis musi zawierać co najmniej precyzyjny czas, typ zdarzenia, identyfikator systemu, numer decyzji (jeżeli dotyczy), kod wyniku.

WF-AU-02 Retrospekcja łańcucha zdarzeń
SOF2 musi udostępniać narzędzie umożliwiające odtworzenie pełnego łańcucha zdarzeń związanych z pojedynczą decyzją, od momentu jej przyjęcia, poprzez rozksięgowanie i aktualizację rozrachunku, aż po wygenerowanie i zaksięgowanie przelewu oraz powiadomienia wysłane do systemu dziedzinowego. Kluczem wyszukiwania jest numer decyzji.

WF-AU-03 Retencja rejestru zdarzeń
Rejestr zdarzeń musi być przechowywany przez okres zgodny z obowiązującymi regulacjami oraz ustaleniami analizy przedwdrożeniowej, nie krótszy niż okres właściwy dla dokumentów księgowych. Mechanizm retencji musi być konfigurowalny.

WF-AU-04 Ochrona integralności zapisów w rejestrze
Zapisy w rejestrze zdarzeń nie mogą być modyfikowane ani usuwane przez Użytkownika. SOF2 musi zabezpieczyć integralność zapisów środkami technicznymi właściwymi dla rejestrów audytowych.

WF-AU-05 Eksport i udostępnianie rejestru do analizy
SOF2 musi umożliwiać uprawnionym Użytkownikom Wewnętrznym wyszukiwanie i eksport zapisów z rejestru zdarzeń na potrzeby analizy, obsługi incydentów oraz kontroli wewnętrznych i zewnętrznych. Eksport musi być dostępny w formatach umożliwiających dalszą obróbkę.

WF-AU-06 Powiązanie rejestru z logiem historii danych
Rejestr zdarzeń operacji międzysystemowych oraz historia zmian danych prowadzona zgodnie z WF-OG-05 muszą być spójne i wzajemnie powiązane. Numer decyzji oraz precyzyjny czas stanowią klucze łączące oba źródła informacji.