Uchwała Nr 1085/2024
Zarządu Województwa Wielkopolskiego
z dnia 19 grudnia 2024 roku

w sprawie: przyjęcia Procedury obsługi zgłoszeń w Service Desk

Na podstawie art. 41 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (t.j. Dz.U. z 2024 r., poz. 566), art. 14li ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (t.j. Dz.U. z 2024 r., poz. 324 ze zm.) oraz § 7 umowy w sprawie powierzenia części zadań związanych z realizacją inwestycji B3.1.1 w ramach planu rozwojowego, Zarząd Województwa Wielkopolskiego uchwala, co następuje:

§ 1

1. Przyjmuje się do stosowania Procedurę obsługi zgłoszeń w Service Desk, która opisuje zasady obsługi zgłoszeń serwisowych Systemu CST2021.
2. Treść procedury stanowi załącznik nr 1 do niniejszej uchwały.

§ 2

Wykonanie uchwały powierza się Dyrektorowi Departamentu Programów Rozwoju Obszarów Wiejskich Urzędu Marszałkowskiego Województwa Wielkopolskiego.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Uzasadnienie
do Uchwały Nr 1085/2024
Zarządu Województwa Wielkopolskiego
z dnia 19 grudnia 2024 roku

w sprawie: przyjęcia Procedury obsługi zgłoszeń w Service Desk

Zgodnie z zawartą 20 września 2024 roku umową z Ministerstwem Rolnictwa i Rozwoju Wsi w sprawie powierzenia części zadań związanych z realizacją inwestycji B3.1.1 w ramach planu rozwojowego, Samorząd Województwa Wielkopolskiego zobowiązany jest do realizacji zadań wynikających z pełnienia roli jednostki wspierającej plan rozwojowy - Krajowy Plan Odbudowy i Zwiększania Odporności.

Zgodnie z art. 14lx ust. 1. ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju dane dotyczące reform są przekazywane przez instytucje odpowiedzialne za realizację reform, a dane dotyczące inwestycji przez instytucje odpowiedzialne za realizację reform lub instytucje odpowiedzialne za realizację inwestycji, do ministra właściwego do spraw rozwoju regionalnego za pośrednictwem systemu teleinformatycznego.

W celu realizacji tego zobowiązania i zagwarantowania odpowiedniej jakości, dokładności i wiarygodności przekazywanych danych wdrażano centralny system teleinformatyczny CST2021. Powyższa procedura przekazana przez Ministerstwo Funduszy i Polityki Regionalnej przedstawia zasady obsługi zgłoszeń serwisowych systemu CST2021, w tym zgłaszania problemów w użytkowaniu aplikacji wchodzących w skład architektury systemu takich jak: SKANER, SL2021 czy WOD2021.

Niniejsza procedura będzie stosowana do wszystkich inwestycji wdrażanych przez Departament Programów Rozwoju Obszarów Wiejskich w ramach Krajowego Plan Odbudowy i Zwiększania Odporności [KPO].

Mając powyższe na uwadze przyjęcie niniejszej uchwały jest uzasadnione.

Załącznik nr 1: Procedura obsługi zgłoszeń w Service Desk

Załącznik nr 1 do uchwały nr 1085/2024 z dnia 19 grudnia 2024 roku

Procedura obsługi zgłoszeń w Service Desk

Wersja 2.2

Z A T W I E R D Z A M

Katarzyna Kromke - Korbel
Zastępca Dyrektora
Departamentu Koordynacji Wdrażania Funduszy Unii Europejskiej

… . . . .

data *podpis*

Historia zmian

Nr	Data	Autorzy	Opis zmian
1.0	18.09.2018	Ministerstwo	Utworzenie nowego dokumentu
1.1	31.07.2020	Ministerstwo	Aktualizacja dokumentu
2.0	20.11.2020	Ministerstwo	Aktualizacja dokumentu
2.1	06.04.2021	Ministerstwo	Aktualizacja dokumentu - uruchomienie produkcyjne SR2021
2.2	26.11.2024	Ministerstwo	Aktualizacja dokumentu

SPIS TREŚCI

1. Wstęp

1.1 Cel

Dokument przedstawia zasady obsługi zgłoszeń serwisowych Systemu. W szczególności dokument ma na celu opisanie procesów, kluczowych ról, świadczonych usług oraz procedur zgłaszania problemów w użytkowaniu aplikacji wchodzących w skład architektury Systemu:

- Administracja
- BK/ BK2021
- E-Kontrole
- Kontrole Krzyżowe
- MWD
- SKANER
- SL2014
- SL2021
- SR2021
- SRHD
- SZT
- SZT2021
- WOD2021

1.2 Odwołania do innych dokumentów

1. Instrukcja obsługi dla użytkownika Service Desk.
2. Regulaminy bezpieczeństwa informacji przetwarzanych w Systemach.

1.3 Wykaz skrótów i definicji

Skrót/Pojęcie	Definicja
Administracja	Aplikacja wchodząca w skład CST2021, opisana w podrozdziale 2.4 Wytycznych na lata 2021-2027.
Administrator merytoryczny, AM I	Wyznaczony pracownik instytucji realizujący zadania określone w rozdziale 7. Wytycznych na lata 2014-2020 oraz w rozdziale 5.2 Wytycznych na lata 2021-2027, Planie Wdrożenia CST2021 dla KPO. Rodzaje AM: • pracownicy Instytucji odpowiedzialnej za Inwestycję/Reformę, powołani do pełnienia funkcji Administratorów Merytorycznych (IOR/IOI); • pracownicy Instytucji Koordynującej, powołani do pełnienia funkcji Administratorów Merytorycznych (AM IK) lub pracownicy tej instytucji wyznaczeni przez AM IK; • pracownicy w Instytucji Zarządzającej programem operacyjnym, powołani do pełnienia funkcji Administratorów Merytorycznych Instytucji Zarządzającej programem operacyjnym (AM IZ); • pracownicy w Instytucji Pośredniczącej (IP) lub Wdrażającej (IW) w ramach programu (operacyjnego) powołani do pełnienia funkcji Administratorów Merytorycznych Instytucji (AM I)

Skrót/Pojęcie	Definicja
Administrator SD	Wyznaczony pracownik Ministerstwa administrujący SD.
Administrator Bezpieczeństwa CST/CST2021 (ABI)	Wyznaczony zgodnie z Polityką Bezpieczeństwa Informacji dla CST/CST2021 pracownik Ministerstwa, w szczególności realizujący zadania związane z koordynacją i obsługą wykrytych lub zgłoszonych podatności i incydentów związanych z bezpieczeństwem informacji przetwarzanych w Systemach.
Baza Wiedzy o Funduszach Europejskich, Baza Wiedzy	System, o którym mowa w *Wytycznych w zakresie informacji i promocji programów operacyjnych polityki spójności na lata 2014-2020.*
Biblioteka CST2021	Podstawowy poziom wsparcia merytorycznego dla perspektywy 2021-2027.
BK/ BK2021	Aplikacja wchodząca w skład CST2021, opisana w podrozdziale 2.7 Wytycznych na lata 2021-2027.
BPB w Ministerstwie	Biuro Polityki Bezpieczeństwa w Ministerstwie.
E-Kontrole	Aplikacja wchodząca w skład CST2021, opisana w podrozdziale 2.8 Wytycznych na lata 2014-2020.
Gestor Systemu	Wyznaczona osoba, odpowiedzialna za zainicjowanie powstania Systemu, ustalenie założeń i funkcjonalności oraz określanie kierunków jego rozwoju.
Incydent związany z bezpieczeństwem informacji	Każde pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działania Systemu i zagrażają lub mogą zagrażać bezpieczeństwu informacji, w tym danych osobowych przetwarzanych w Systemie. Również zdarzenie umożliwiające uzyskanie jakiegokolwiek nieautoryzowanego dostępu do Systemów.
Instytucja (lub właściwa instytucja)	IK, IZ, IP, IW lub inna instytucja zaangażowana w realizację programów operacyjnych w perspektywie finansowej 2014-2020 oraz 2021-2027, która posiada dostęp do Systemu, nadany zgodnie z Wytycznymi. W przypadku KPO są to także IOR/IOI.
IOD w Ministerstwie	Inspektor Ochrony Danych Osobowych w Ministerstwie.
Kontrole Krzyżowe	Aplikacja wchodząca w skład CST2021, opisana w podrozdziale 2.11 Wytycznych na lata 2021-2027.
Ministerstwo	Urząd administracji rządowej obsługujący ministra właściwego do spraw rozwoju regionalnego.

Skrót/Pojęcie	Definicja
Modyfikacja danych	Edycja danych wprowadzonych do SL2014 i CST2021, zablokowanych do edycji z poziomu użytkownika, które zostały zarejestrowane jako zgłoszenie modyfikacji danych w zakresie zgodnym z załącznikiem nr 2. Również modyfikacje danych powstałe w wyniku wykonania skryptu modyfikującego dane.
Pełnomocnik do spraw SZBI dla CST/ CST2021	Wyznaczona na mocy Polityki Bezpieczeństwa Informacji dla CST/ CST2021 osoba, sprawująca nadzór nad wdrożonym Systemem Zarządzania Bezpieczeństwem Informacji (SZBI) dla CST/CST2021.
Pierwszy poziom wsparcia	AM, do którego bezpośrednio zwraca się Użytkownik.
Podatność	Luka (słabość) aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w Systemie.
Problem merytoryczny	Wadliwe merytorycznie działanie Systemu, niezgodne z opisem wymagań określonych w dokumentacji dotyczącej Systemu (m.in. w instrukcjach użytkownika). W ramach Problemu merytorycznego może być również zgłaszana potrzeba utworzenia/modyfikacji raportu w SRHD/SR2021.
Problem obsługowy	Problem związany z obsługą lub użytkowaniem Systemu.
Problem technicznym	Problem związany z: • nieprawidłowym technicznym działaniem Systemu lub • nieprawidłowym działaniem stacji roboczej Użytkownika lub • nieprawidłowym działaniem sieci Użytkownika-I lub • nieprawidłowym działaniem mechanizmu automatycznej wymiany danych między systemami lub inny problem nie będący problemem merytorycznym lub obsługowym.
Raport z obsługi	Raport z obsługi podatności, zdarzenia lub incydentu związanego z przetwarzaniem danych osobowych w CST/CST2021 zawierający szczegółowe informacje dotyczące sposobu obsługi, przyczyn, zakresu, skutków oraz zastosowanych działań zaradczych.
SD	Aplikacja Service Desk dla Systemu. Dostępny przez sieć Internet system informatyczny, umożliwiający rejestrację zgłoszeń, zarządzany i udostępniany przez Ministerstwo.
SKANER	Aplikacja wchodząca w skład CST2021, opisana w podrozdziale 2.10 Wytycznych na lata 2021-2027.
SL2014	Aplikacja główna Centralnego Systemu Teleinformatycznego opisana w podrozdziale 3 rozdziału 5 Wytycznych na lata 2014-2020, wspierająca realizację programów operacyjnych współfinansowanych ze środków UE w perspektywie finansowej 2014-2020.
SL2021	Aplikacja wchodząca w skład CST2021, opisana w podrozdziale 2.6 Wytycznych na lata 2021-2027. System wspierający realizację programów operacyjnych współfinansowanych ze środków UE w perspektywie finansowej 2021-2027.

Skrót/Pojęcie	Definicja
Służby informatyczne w Instytucji Administratora Merytorycznego IOR IOI/I/IZ/IK	Jednostki organizacyjne zajmujące się obsługą informatyczną w instytucji, w której pracuje Administrator Merytoryczny obsługujący lub zgłaszający problem.
SR2021	Aplikacja wchodząca w skład CST2021, opisana w podrozdziale 2.9 Wytycznych na lata 2021-2027.
SRHD	Aplikacja raportująca Centralnego systemu teleinformatycznego oparta na hurtowni danych, umożliwiająca generowanie raportów na podstawie danych zgromadzonych w SL2014; opisana w podrozdziale 4 rozdziału 5 Wytycznych na lata 2014-2020.
System	Centralny system teleinformatyczny, o którym mowa w rozdziale 16 ustawy z dnia 11 lipca 2014 r. *o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020* (Dz. U. z 2020 r. poz. 818) lub System, o którym mowa w art. 4 ust. 2 pkt 6 ustawy z dnia 28 kwietnia 2022 r. *o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej* (Dz. U. z Dz.U. 2022 poz. 1079) – odpowiednio: Centralny system teleinformatyczny (CST), Centralny system teleinformatyczny 2021 (CST2021).
SZT	System zarządzania tożsamością – aplikacja wspierająca zarządzanie procesami logowania w ramach Centralnego systemu teleinformatycznego opisana w podrozdziale 5 rozdziału 5 Wytycznych na lata 2014-2020.
SZT2021	Aplikacja wchodząca w skład CST2021, opisana w podrozdziale 2.3 Wytycznych na lata 2021-2027.
Użytkownik	Osoba mająca dostęp do co najmniej jednej z aplikacji wchodzących w skład Systemów.
WOD2021	Aplikacja wchodząca w skład CST2021, opisana w podrozdziale 2.5 Wytycznych na lata 2021-2027.
Wykonawca	Podmiot obsługujący zgłoszenia na podstawie umowy zawartej z Ministerstwem.
Wytyczne na lata 2014-2020/ Wytyczne na lata 2021-2027	*Wytyczne w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020* oraz *Wytyczne w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2021-2027.*
Zapytanie	Zgłoszenie Użytkownika do pierwszego poziomu wsparcia, na które pierwszy poziom wsparcia udzielił natychmiast odpowiedzi (bez przesyłania do kolejnej linii wsparcia). Zapytania nie są ewidencjonowanie w SD.
Zdarzenie związane z bezpieczeństwem informacji	Stan Systemu, usługi lub sieci, wskazujący na możliwe naruszenie Regulaminu bezpieczeństwa informacji przetwarzanych w Systemach, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem. Każde zdarzenie, które może wskazywać na próby naruszenia polityki bezpieczeństwa informacji, procedur, standardów.
Zgłoszenie	To: • informacja o wystąpieniu utrudnienia lub braku możliwości wykorzystania funkcjonalności Systemu lub systemów wspierających, • prośba o wyjaśnienie problemu, • prośba o modyfikację danych, • prośba o utworzenie/modyfikację raportu w SRHD/SR2021 • informacja o zdarzeniu związanym z bezpieczeństwem informacji

Skrót/Pojęcie	Definicja
	• żądanie przywrócenia poprawności działania Systemu lub systemów wspierających przekazane przez Użytkownika i zarejestrowane w SD, • drobne prace programistyczne (DPP).
Zmiana w Systemie	Uzasadniona propozycja zmiany funkcjonalności Systemu zarejestrowana w SD.

1.4 Zakres dokumentu

Dokument ma zastosowanie do działań związanych z rozwiązywaniem problemów z eksploatacją Systemu:

- obsługowych, związanych z użytkowaniem Systemu;
- technicznych, związanych z brakiem możliwości uruchomienia Systemu, z niemożnością nawiązania połączenia itp.,
- merytorycznych, związanych z przyjętymi założeniami merytorycznymi działania Systemu i zgromadzonymi w nim danymi,
- dotyczących sytuacji zagrożenia bezpieczeństwa informacji przetwarzanych w Systemie w tym zgłoszeń związanych z ochroną danych osobowych,

a także zbieraniem i zarządzaniem propozycjami zmian w Systemie.

2. Dostęp do SD

Dostępem do SD zarządza Administrator SD

Administratorzy merytoryczni otrzymują dostęp do SD zgodny z poziomem w strukturze wdrażania, login jest tworzony na podstawie roli i instytucji (np. AM_IP26_POIS). Na potrzeby komunikacji z SD Instytucja udostępnia adres e-mail o składni: [nadany login] @ [domena instytucji].

W przypadku konieczności zmiany hasła należy skorzystać z funkcjonalności dostarczanej przez system SD: *Nie możesz się zalogować?*

Funkcjonalność pozwala na wysłanie wiadomości na adres mailowy użytkownika zarejestrowany w systemie SD, w której znajdują się informacje umożliwiające zalogowanie do SD.

3. Zgłoszenia

SD zapewnia odpowiednie rozwiązania organizacyjne i techniczne umożliwiające obsługę zgłoszeń dot. Systemu, w szczególności umożliwia:

a) przeprowadzenie analizy zgłoszenia oraz opracowanie rozwiązania wyeliminowania problemu/błędu,

b) przydzielenie osoby do obsługi zgłoszenia,

c) obsługę zgłoszeń przekazanych przez AM,

d) natychmiastowe rozwiązywanie prostych problemów i zapytań,

e) Obsługę incydentów bezpieczeństwa oraz naruszeń danych osobowych.

Minimalny zakres danych stanowiących podstawę obsługi zgłoszenia, to:

1. Nazwa aplikacji
2. Login użytkownika
3. Opis problemu
4. Numer projektu (jeżeli dotyczy)
5. Rodzaj dokumentu (jeżeli dotyczy konkretnego dokumentu w ramach projektu)
6. Nazwa/numer identyfikacyjny dla dokumentu (jeżeli dotyczy konkretnego dokumentu w ramach projektu)
7. Jeżeli zgłaszane jest powodowane wystąpienie błędu (komunikatu z błędem, błędu na stronie np. 504):
    a. Identyfikator błędu (jeżeli użytkownik posiada)
    b. Data i godzinę wystąpienia błędu
    c. Kod instancji aplikacji, na której wystąpił błąd (jeżeli użytkownik posiada)
    d. Podstawowe kroki prowadzące do wystąpienia błędu
8. Rodzaj i wersja przeglądarki
9. Ewentualne zrzuty ekranu

3.1 Rodzaje zgłoszeń

a) zapytania - udzielanie wyjaśnień Użytkownikom dotyczących obsługi Systemu bez rejestracji w SD,

b) problemy merytoryczne (w tym prośba o utworzenie/modyfikację raportu w SRHD/SR2021), obsługowe i techniczne (przyjmowanie zgłoszeń dotyczących niepoprawnej pracy Systemu),

c) zmiany w Systemie,

d) zdarzenia, incydenty i podatności związane z bezpieczeństwem informacji,

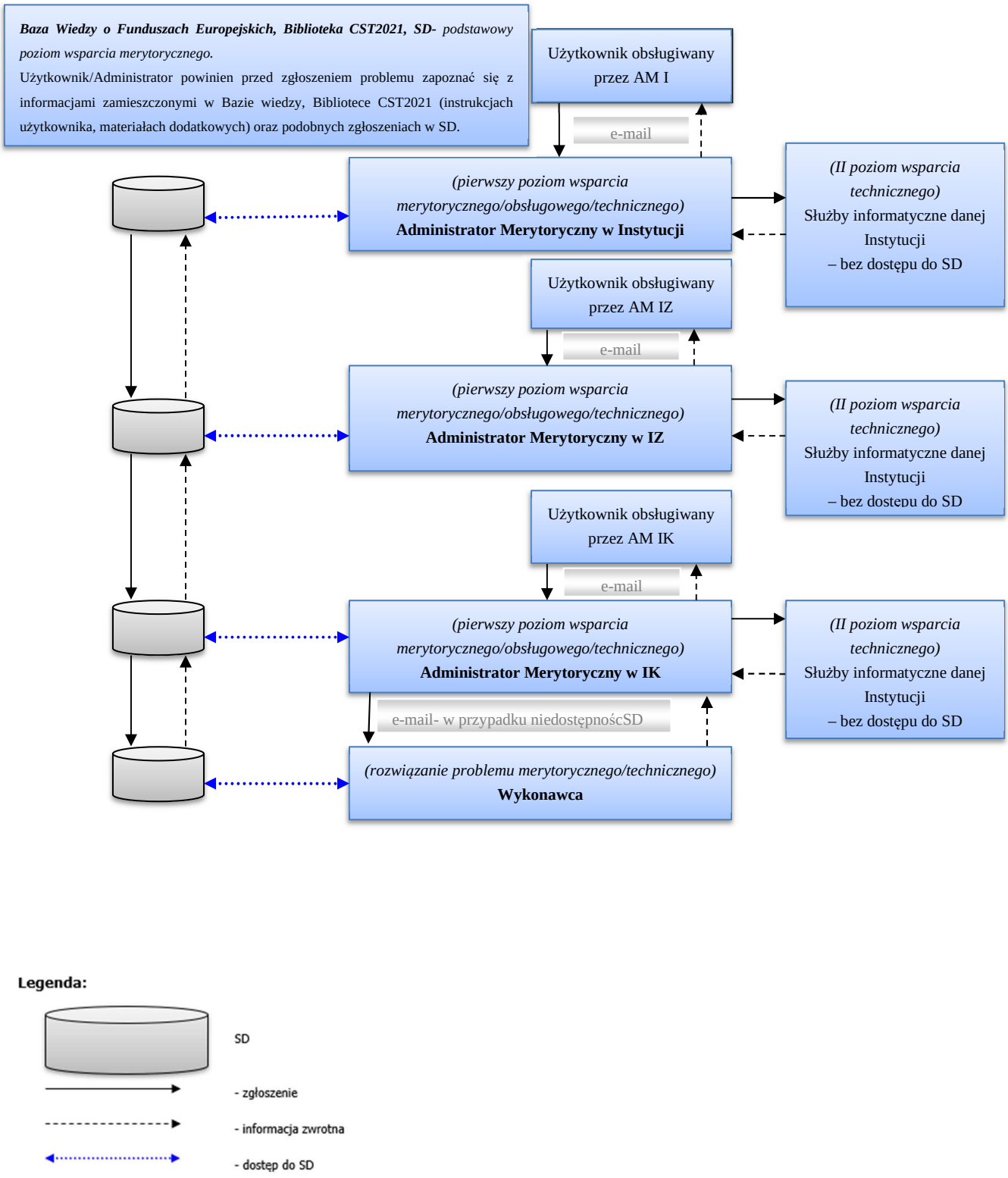
e) modyfikacja danych,

f) obsługa zgłoszeń dot. problemu braku możliwości terminowego przedłożenia danych w Systemie

Poniższe diagramy i tabele przedstawiają procedury obsługi poszczególnych rodzajów zgłoszeń:

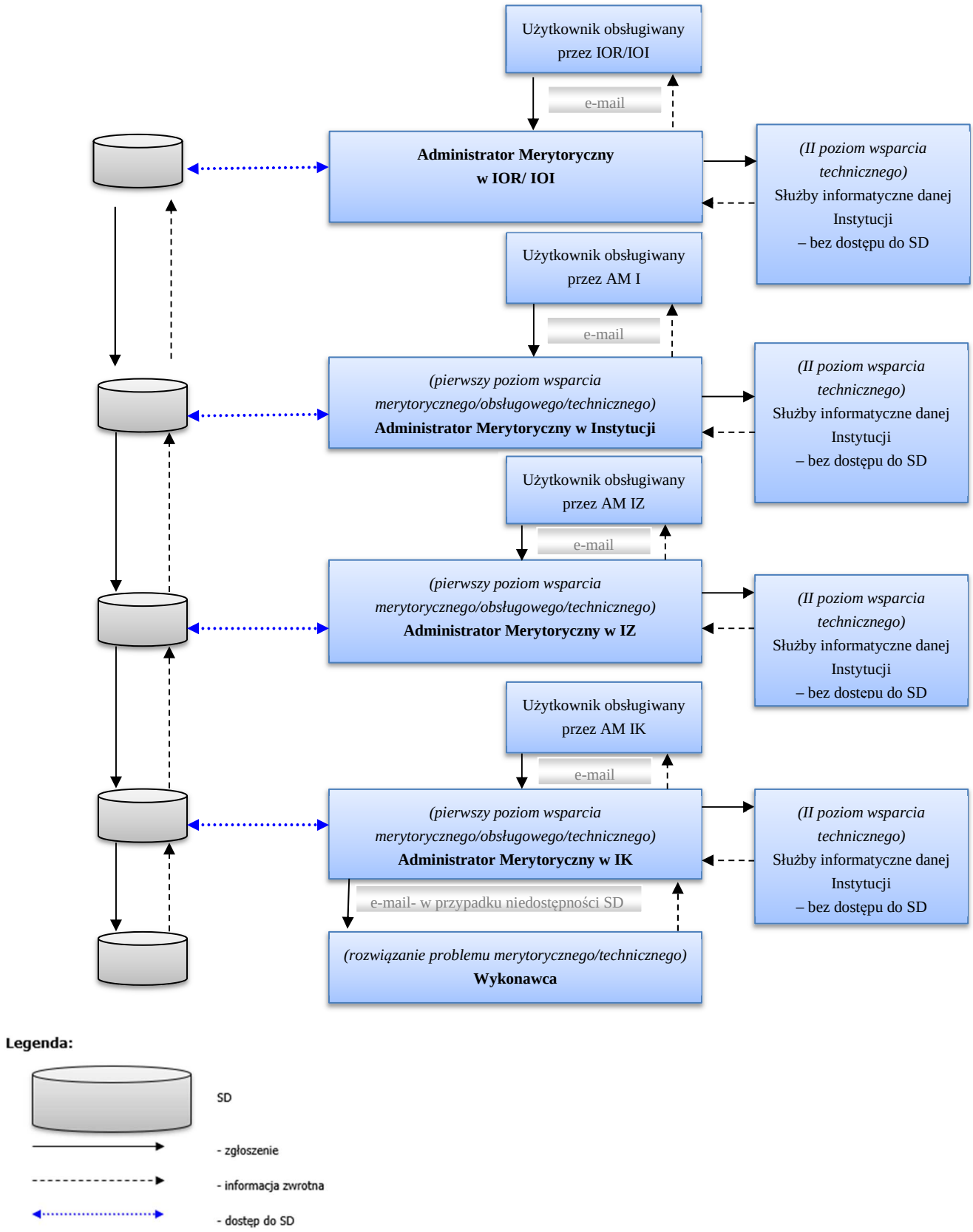
3.2 Obsługa zgłoszeń

3.2.1 Diagram procedury – Programy inne niż Krajowy Plan Odbudowy i Wspierania Odporności



Legenda:

3.2.2 Diagram procedury - Krajowy Plan Odbudowy i Wspierania Odporności



Role i zadania

Rola	***Zadania***
Użytkownik	W przypadku stwierdzenia problemu Użytkownik przegląda Bazę wiedzy o funduszach europejskich lub Bibliotekę CST2021. Jeśli nie znajdzie rozwiązania problemu lub odpowiedzi: a) opracowuje zgłoszenie problemu poprzez wypełnienie „Formularza zgłaszania problemów" przedstawionego w Załączniku nr 1 do niniejszego dokumentu, b) przesyła wypełniony formularz pocztą elektroniczną do właściwego Administratora Merytorycznego
	Przykład problemu obsługowego: Użytkownik zgłasza się z pytaniem jak wypełnić daną formatkę. *Przykład problemu merytorycznego: W systemie niewłaściwie wyliczane (sumowane) są dane liczbowe.* *Przykład problemu technicznego: Brak możliwości zalogowania się do Systemu spowodowany nieprawidłową konfiguracją przeglądarki internetowej.*
[dla zgłoszeń dot. Krajowego Planu Odbudowy i Wspierania Odporności] **Administrator Merytoryczny w IOR/IOI**	Otrzymuje zgłoszenie od Użytkownika pocztą elektroniczną (następnie je archiwizuje). a) przeprowadza analizę zgłoszenia– sprawdza w bazie zgłoszeń SD czy podobne zgłoszenie nie było już obsługiwane oraz weryfikuje, czy przyczyną zgłoszenia nie są problemy lokalne, co potwierdza u własnych służb informatycznych. b) jeśli może sam udzielić właściwej odpowiedzi, to przesyła ją Użytkownikowi za pomocą poczty elektronicznej (UWAGA: w takim przypadku odpowiedź nie jest rejestrowana w SD, dlatego sugeruje się archiwizowanie informacji/odpowiedzi przesłanych pocztą elektroniczną) c) jeżeli zgłoszenie jest zasadne i AM IOR/IOI nie może sam udzielić właściwej odpowiedzi, rejestruje zgłoszenie w SD, d) dołącza w SD do zgłoszenia „Formularz zgłaszania problemów w Systemie i jeśli to konieczne, bardziej szczegółowy opis problemu, e) w uzasadnionych przypadkach, po analizie zgłoszenia, może odrzucić zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie problemu zmienia wtedy status na zamknięte), f) jeśli nie potrafi rozwiązać problemu, to przekazuje zgłoszenie na poziom Administratora Merytorycznego Instytucji, podając przy tym przyczynę przekazania, g) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia, zamyka zgłoszenia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji,
Administrator Merytoryczny w Instytucji	Otrzymuje zgłoszenie od Użytkownika pocztą elektroniczną (następnie je archiwizuje). a) przeprowadza analizę zgłoszenia– sprawdza w bazie zgłoszeń SD czy podobne zgłoszenie nie było już obsługiwane oraz weryfikuje, czy przyczyną zgłoszenia nie są problemy lokalne, co potwierdza u własnych służb informatycznych.

Rola	***Zadania***
	b) jeśli może sam udzielić właściwej odpowiedzi, to przesyła ją Użytkownikowi za pomocą poczty elektronicznej (UWAGA: w takim przypadku odpowiedź nie jest rejestrowana w SD, dlatego sugeruje się archiwizowanie informacji/odpowiedzi przesłanych pocztą elektroniczną) jeżeli zgłoszenie jest zasadne i AM I nie może sam udzielić właściwej odpowiedzi, rejestruje zgłoszenie w SD, c) dołącza w SD do zgłoszenia „Formularz zgłaszania problemów w Systemie i jeśli to konieczne, bardziej szczegółowy opis problemu, d) w uzasadnionych przypadkach, po analizie zgłoszenia, może odrzucić zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie problemu zmienia wtedy status na zamknięte), e) jeśli nie potrafi rozwiązać problemu, to przekazuje zgłoszenie na poziom Administratora Merytorycznego w IZ, podając przy tym przyczynę przekazania, f) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia, zamyka zgłoszenia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, g) informuje Użytkownika o zamknięciu zgłoszenia – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości) Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „AMI_Zamknięte” AMI tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie” AMI_zamknięte”.
	W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych IOR / IOI: a) przeprowadza analizę zgłoszenia – sprawdza w SD czy podobne zgłoszenie nie było już obsługiwane. W wyniku analizy AM I może cofnąć zgłoszenie do IOR / IOI; weryfikuje zgłoszenie pod kątem załączenia kompletnych danych potrzebnych do analizy i zgodności z niniejszą procedurą, modyfikując zgłoszenie, jeśli tego wymaga; b) jeśli nie może sam udzielić właściwej odpowiedzi, to podaje przyczynę przekazania, a następnie przekazuje zgłoszenie na poziom Administratora Merytorycznego w IZ, załączając wynik analizy z pkt a; c) jeśli zgłoszenie nie jest zasadne - odrzuca je, podając przy tym przyczynę odrzucenia, d) jeśli zgłoszenie wymaga uzupełnienia - cofa zgłoszenie do IOR/ IOI, e) jeśli potrafi rozwiązać problem samodzielnie, to rozwiązuje problem i przekazuje je do weryfikacji na niższym poziomie wsparcia, f) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji. Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „AM IZ_Zamknięte” AM IZ tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie ”AM IZ_zamknięte”.

Rola	***Zadania***
Służby informatyczne Instytucji Użytkownika	(drugi poziom wsparcia technicznego) a) otrzymują zgłoszenie dot. problemu technicznego od Administratora Merytorycznego, b) udzielają odpowiedzi.
Administrator Merytoryczny w IZ	**W przypadku zgłoszeń otrzymanych od Użytkowników z IZ:** Otrzymuje zgłoszenie od Użytkownika pocztą elektroniczną (następnie je archiwizuje). a) przeprowadza analizę zgłoszenia – sprawdza w SD lub dokonuje weryfikacji czy podobne zgłoszenie nie było już obsługiwane. b) jeśli może sam udzielić właściwej odpowiedzi, to przesyła ją Użytkownikowi za pomocą poczty elektronicznej (UWAGA: w takim przypadku odpowiedź nie jest rejestrowana w SD, dlatego sugeruje się archiwizowanie informacji/ odpowiedzi przesłanych pocztą elektroniczną), c) jeżeli zgłoszenie jest zasadne i nie może sam udzielić właściwej odpowiedzi, rejestruje zgłoszenie w SD (jeśli zgłoszenie dotyczy problemu technicznego kontaktuje się dodatkowo z własnymi służbami informatycznymi), d) jeśli konieczne, to dołącza w SD do zgłoszenia załączniki i szczegółowy opis problemu, e) w uzasadnionych przypadkach, po analizie zgłoszenia, może odrzucić zgłoszenie w SD podając przy tym przyczynę odrzucenia (zgłoszenie problemu zmienia wtedy status na zamknięte), f) jeśli nie potrafi rozwiązać problemu, to przekazuje zgłoszenie na poziom Administratora Merytorycznego w IK, podając przy tym przyczynę przekazania i załączając wynik analizy z pkt a, g) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia, zamyka zgłoszenia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, h) informuje Użytkownika o zakończeniu realizacji zgłoszenia – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości).

Rola	***Zadania***
	W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych Instytucji niższego poziomu: a) przeprowadza analizę zgłoszenia – sprawdza w SD, Bazie wiedzy lub Bibliotece CST2021 czy podobne zgłoszenie nie było już obsługiwane. W wyniku analizy AM IZ może cofnąć zgłoszenie do AMI; weryfikuje zgłoszenie pod kątem załączenia kompletnych danych potrzebnych do analizy i zgodności z niniejszą procedurą, modyfikując zgłoszenie, jeśli tego wymaga; b) jeśli nie może sam udzielić właściwej odpowiedzi, to podaje przyczynę przekazania, a następnie przekazuje zgłoszenie na poziom Administratora Merytorycznego w IK, załączając wynik analizy z pkt a; c) jeśli zgłoszenie nie jest zasadne - odrzuca je, podając przy tym przyczynę odrzucenia, d) jeśli zgłoszenie wymaga uzupełnienia - cofa zgłoszenie do AMI, e) jeśli potrafi rozwiązać problem samodzielnie, to rozwiązuje problem iprzekazuje je do weryfikacji na niższym poziomie wsparcia, f) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, g) przekazuje zgłoszenia do weryfikacji na poziomie AMI. Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „AM IZ_Zamknięte” AM IZ tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie ”AM IZ_zamknięte”.

Rola	***Zadania***
Administrator Merytoryczny w IK	**W przypadku zgłoszeń otrzymanych od Użytkowników z IK:** Otrzymuje zgłoszenie od Użytkownika pocztą elektroniczną (następnie je archiwizuje). a) przeprowadza analizę zgłoszenia – sprawdza w SD czy podobne zgłoszenie nie było już obsługiwane. b) jeśli może sam udzielić właściwej odpowiedzi, to przesyła ją Użytkownikowi za pomocą poczty elektronicznej (UWAGA: w takim przypadku odpowiedź nie jest rejestrowana w SD, dlatego sugeruje się archiwizowanie informacji/odpowiedzi przesłanych pocztą elektroniczną), c) jeżeli zgłoszenie jest zasadne i nie może sam udzielić właściwej odpowiedzi, rejestruje zgłoszenie w SD, d) jeśli konieczne, to dołącza w SD do zgłoszenia załączniki i szczegółowy opis problemu, e) w uzasadnionych przypadkach, po analizie zgłoszenia, może odrzucić zgłoszenie w SD podając przy tym przyczynę odrzucenia(zgłoszenie problemu zmienia wtedy status na zamknięte), f) w uzasadnionych przypadkach, po analizie zgłoszenia, może zamrozić zgłoszenie w celu jego późniejszej realizacji. g) jeśli nie potrafi rozwiązać problemu, to przekazuje zgłoszenie do Wykonawcy oprogramowania, h) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia, zamyka zgłoszenia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji bądź uzupełnienia informacji niezbędnych do obsługi zgłoszenia i) informuje Użytkownika o zakończeniu realizacji zgłoszenia – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości). Uwaga: AM IK może ponownie otworzyć zgłoszenie problemu, które posiada status „IK_Zamknięte”.

Rola	***Zadania***
	W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych Instytucji niższego poziomu: a) przeprowadza analizę zgłoszenia – sprawdza w SD czy podobne zgłoszenie nie było już obsługiwane. W wyniku analizy AM IK może cofnąć zgłoszenie do AM IZ, weryfikuje zgłoszenie pod kątem załączenia kompletnych danych potrzebnych do analizy i zgodności z niniejszą procedurą, modyfikując zgłoszenie, jeśli tego wymaga; b) jeśli nie może sam udzielić właściwej odpowiedzi, to podaje przyczynę przekazania, a następnie przekazuje zgłoszenie do Wykonawcy oprogramowania, c) jeśli zgłoszenie nie jest zasadne - odrzuca je, d) w uzasadnionych przypadkach, po analizie zgłoszenia, może zamrozić zgłoszenie w celu jego późniejszej realizacji, e) jeśli zgłoszenie wymaga uzupełnienia - cofa zgłoszenie do AM IZ, f) jeśli potrafi rozwiązać problem samodzielnie, to rozwiązuje problem i przekazuje je do weryfikacji na niższym poziomie wsparcia, g) weryfikuje sposób realizacji zgłoszenia na poziomie Wykonawcy lub przekazuje je do ponownej realizacji w przypadku jego reklamacji bądź uzupełnienia informacji niezbędnych do obsługi zgłoszenia, h) przekazuje zgłoszenia do weryfikacji na poziomie AM IZ. Uwaga: AM IK może ponownie otworzyć zgłoszenie problemu, które posiada status „IK_Zamknięte”.
Wykonawca	Obsługuje zgłoszenie dot. problemu merytorycznego/technicznego w SD: a) realizuje zgłoszenie, b) proponuje odrzucenie zgłoszenia w SD, podając przy tym przyczynę odrzucenia, c) przekazuje informacje o infrastrukturze, wskazuje elementy, które powodują błąd oraz wszelkie informacji o Systemach potrzebnych do przywrócenia ich pełnej funkcjonalności, d) cofa zgłoszenie na niższy poziom w celu jego uzupełnienia.

3.2.3 Ścieżka przepływu zgłoszeń

Użytkownik obsługiwany przez IOR / IOI ↔ Administrator Merytoryczny w IOIR IOI ↔ Administrator Merytoryczny w Instytucji ↔Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny IK↔Wykonawca.

Użytkownik obsługiwany przez AM I↔ Administrator Merytoryczny w Instytucji ↔Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny IK↔Wykonawca.

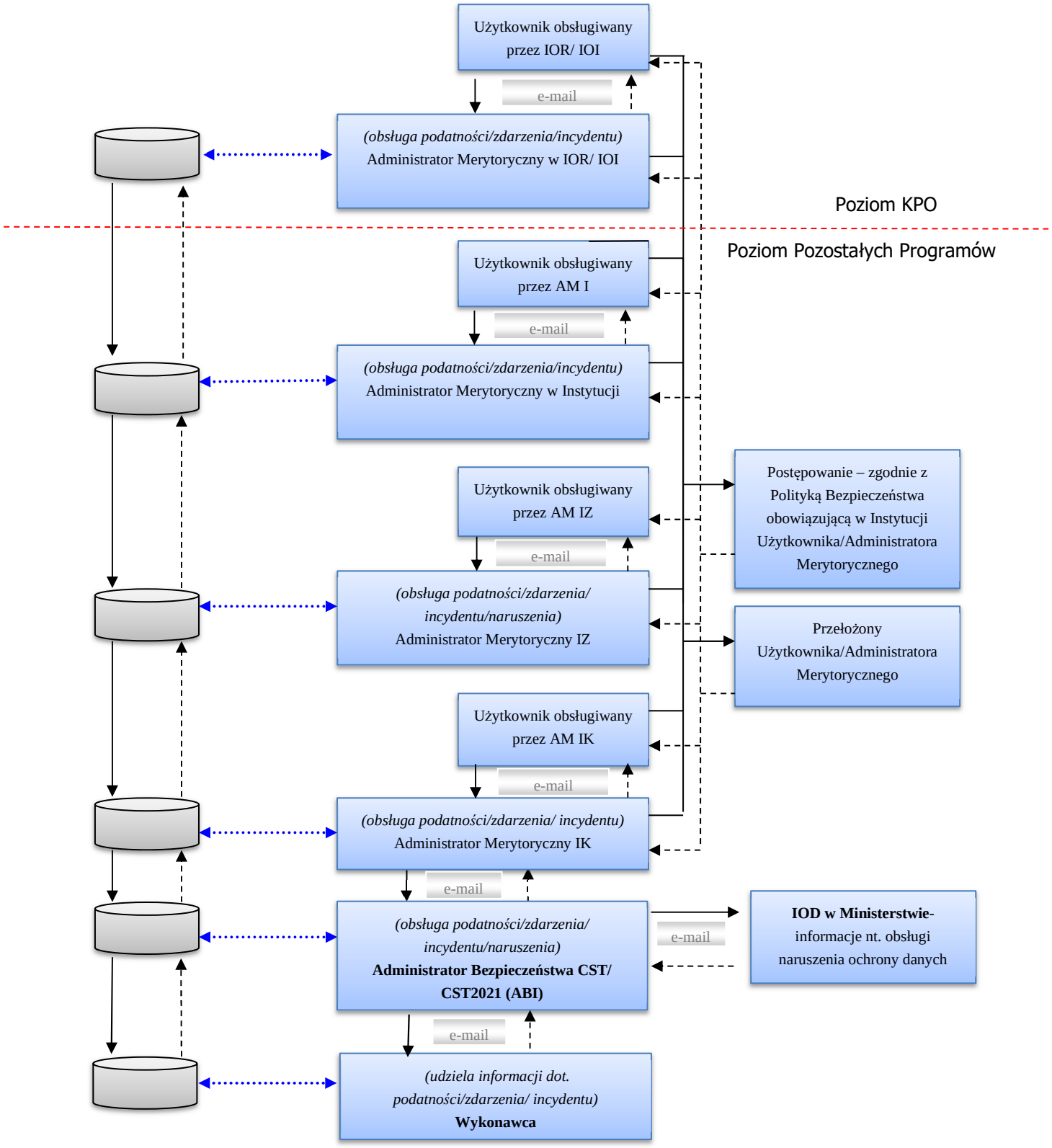
Użytkownik obsługiwany przez AM IZ↔ Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny w IK↔Wykonawca.

Użytkownik obsługiwany przez AM IK↔ Administrator Merytoryczny w IK↔Wykonawca.

3.3 Zgłoszenie podatności, zdarzenia lub incydentu dotyczącego bezpieczeństwa informacji (w tym podatności, zdarzenia lub incydentu związanego z przetwarzaniem danych osobowych)

3.3.1 Diagram procedury

POSTĘPOWANIE W SYTUACJI STWIERDZENIA PODATNOŚCI, ZDARZENIA LUB INCYDENTU DOTYCZĄCEGO BEZPIECZEŃSTWA INFORMACJI LUB PRZETWARZANIA DANYCH OSOBOWYCH



Role i zadania

Rola	***Zadania***
Użytkownik	a) Postępuje zgodnie z Regulaminami bezpiecznego użytkowania Systemu, którego dotyczy zgłoszenie. b) Po stwierdzeniu wystąpienia lub podejrzeniu wystąpienia naruszenia bezpieczeństwa informacji w Systemie Użytkownik powinien: • Powstrzymać się od wszelkich czynności mogących zatrzeć ślady naruszenia bezpieczeństwa informacji, • Powstrzymać się od wszelkich działań w systemie, zwłaszcza od usuwania podejrzanego oprogramowania, • Powiadomić za pomocą poczty elektronicznej Administratora Merytorycznego o sytuacji zagrożenia bezpieczeństwa informacji, c) Po zgłoszeniu zagrożenia do Administratora Merytorycznego, zastosować się do jego poleceń, o ile nie są one niezgodne z Polityką Bezpieczeństwa obowiązującą w Instytucji Użytkownika, d) Przekazać informacje o zagrożeniu, jeśli zostanie o to poproszony przez ABI.
[dla zgłoszeń dot. Krajowego Planu Odbudowy i Wspierania Odporności] **Administrator Merytoryczny w IOR/IOI**	a) Otrzymuje od Użytkownika pocztą elektroniczną (następnie je archiwizuje) zgłoszenie dot. podatności, zdarzenia, incydentu lub incydentu związanego z przetwarzaniem danych osobowych, b) Weryfikuje poprawność typu zgłoszenia. Jeśli nie jest to zgłoszenie dotyczące bezpieczeństwa informacji, to zmienia typ zgłoszenia na właściwy i postępuje zgodnie z procedurami opisanymi w punkcie 3.2, c) Jeśli jest to zgłoszenie dot. bezpieczeństwa informacji, to Administrator Merytoryczny w IOR/ IOI powinien: • Potwierdzić czy zgłoszenie bezpieczeństwa rzeczywiście miało miejsce i czy zostało właściwie zakwalifikowane przez zgłaszającego, • Ustalić, czy istnieje zagrożenie dla funkcjonowania Systemu, • Ustalić, czy komputer powinien zostać odizolowany od sieci; jeśli tak, to poinformować o tym ABI w Instytucji (jeżeli jest wyznaczony) oraz kierującą komórką informatyczną danej Instytucji, • Zabezpieczyć dowody zdarzenia, • Zlecić użytkownikowi dalszy sposób postępowania d) Rejestruje zgłoszenie w SD i przesyła na poziom Administratora Merytorycznego w Instytucji. W przypadku braku dostępności SD, Administrator Merytoryczny w IOR/IOI dokona zgłoszenia na adres cst@mfipr.gov.pl. Zgłoszenie dotyczące incydentu należy oznaczy w tytule wiadomości, w nawiasie kwadratowym słowem „[INCYDENT]". e) Informuje Użytkownika o zamknięciu zgłoszenia – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości), f) Sporządza notatkę o zagrożeniu, jeśli zostanie o to poproszony przez ABI oraz stosuje się do zaleceń wydanych przez ABI.

	W przypadku podatności, zdarzenia lub incydentu dotyczącego przetwarzania danych osobowych związanych z CST2021, jeśli naruszenie nie jest spowodowane nieprawidłowym działaniem Systemu, Administrator dokonuje oceny naruszenia i postępuje zgodnie z rozporządzeniem RODO, ustawą o ochronie danych osobowych oraz wewnętrznymi procedurami Instytucji.
Administrator Merytoryczny w Instytucji	a) Otrzymuje od Użytkownika pocztą elektroniczną (następnie je archiwizuje) zgłoszenie dot. podatności, zdarzenia, lub incydentu, b) Weryfikuje poprawność typu zgłoszenia. Jeśli nie jest to zgłoszenie dotyczące bezpieczeństwa informacji, to zmienia typ zgłoszenia na właściwy i postępuje zgodnie z procedurami opisanymi w punkcie 3.2, c) Jeśli jest to zgłoszenie dot. bezpieczeństwa informacji, to AM I powinien: Potwierdzić, czy zagrożenie bezpieczeństwa rzeczywiście miało miejsce i czy zostało właściwie zakwalifikowane przez zgłaszającego, • Ustalić, czy istnieje zagrożenie dla funkcjonowania Systemu, • Ustalić, czy komputer powinien zostać odizolowany od sieci; jeśli tak, to poinformować o tym ABI w Instytucji (jeżeli jest wyznaczony) oraz osobę kierującą komórką informatyczną w danej Instytucji, • Zabezpieczyć dowody zdarzenia, • Zalecić Użytkownikowi sposób dalszego postępowania lub, jeśli podejrzenie naruszenia bezpieczeństwa nie zostało potwierdzone, poinformować go o możliwości kontynuowania pracy. d) Rejestruje podatność, zdarzenie lub incydent w SD i przesyła na poziom IZ. W przypadku braku dostępności SD, AM I dokonuje zgłoszenia pocztą elektroniczną na adres cst@mfipr.gov.pl. Zgłoszenie dotyczące incydentu należy oznaczy w tytule wiadomości, w nawiasie kwadratowym słowem „[INCYDENT]”. e) Informuje Użytkownika o zamknięciu zgłoszenia – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości), f) Sporządza notatkę o zagrożeniu, jeśli zostanie o to poproszony przez ABI oraz stosuje się do zaleceń wydanych przez ABI.
	W przypadku podatności, zdarzenia lub incydentu dotyczącego przetwarzania danych osobowych związanych z CST2021, jeśli naruszenie nie jest spowodowane nieprawidłowym działaniem Systemu, Administrator dokonuje oceny naruszenia i postępuje zgodnie z rozporządzeniem RODO, ustawą o ochronie danych osobowych oraz wewnętrznymi procedurami Instytucji.

	W przypadku zgłoszeń incydentów przesyłanych w SD przez Administratorów Merytorycznych niższego poziomu: W przypadku przekazania na poziom AM I w SD zgłoszenia podatności, zdarzenia lub incydentu przez IOR/ IOI, przesyła zgłoszenie na poziom IZ.
Służby informatyczne Instytucji Użytkownika	a) Otrzymują zgłoszenie dot. zagrożenia bezpieczeństwa informacji od Administratora Merytorycznego, b) Udzielają odpowiedzi/podejmują działanie.
Administrator Merytoryczny w IZ	**W przypadku zgłoszeń podatności, zdarzeń lub incydentów otrzymanych od Użytkowników z IZ:** a) Otrzymuje od Użytkownika pocztą elektroniczną (następnie je archiwizuje) zgłoszenie dot. podatności, zdarzenia lub incydentu, b) Weryfikuje poprawność typu zgłoszenia. Jeśli nie jest to zgłoszenie dotyczące bezpieczeństwa informacji, to zmienia typ zgłoszenia na właściwy i postępuje zgodnie z procedurami opisanymi w punkcie3.2, c) Jeśli jest to zgłoszenie dot. bezpieczeństwa informacji, AM IZ powinien: • Potwierdzić, czy zagrożenie bezpieczeństwa rzeczywiście miało miejsce i czy zostało właściwie zakwalifikowane przez zgłaszającego jako podatność, zdarzenie lub incydent, • Ustalić, czy istnieje zagrożenie dla funkcjonowania Systemu, • Ustalić, czy komputer powinien zostać odizolowany od sieci; jeśli tak, to poinformować o tym ABI w Instytucji (jeżeli jest wyznaczony) oraz osobę kierującą komórką informatyczną w danej Instytucji, • Zabezpieczyć dowody zdarzenia, • Zalecić Użytkownikowi sposób dalszego postępowania lub, jeśli podejrzenie naruszenia bezpieczeństwa nie zostało potwierdzone, poinformować go o możliwości kontynuowania pracy. d) Rejestruje podatność, zdarzenie lub incydent w SD. W przypadku braku dostępności SD AM IZ dokonuje zgłoszenia pocztą elektroniczną na adres cst@mfipr.gov.pl. Zgłoszenie dotyczące incydentu należy oznaczy w tytule wiadomości, w nawiasie kwadratowym słowem „[INCYDENT]". e) Informuje Użytkownika o zamknięciu zgłoszenia – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości), f) Sporządza notatkę o zagrożeniu, jeśli zostanie o to poproszony przez ABI oraz stosuje się do zaleceń wydanych przez ABI.
	W przypadku podatności, zdarzenia lub incydentu dotyczącego przetwarzania danych osobowych związanych z CST2021, jeśli naruszenie nie jest spowodowane nieprawidłowym działaniem Systemu, Administrator dokonuje oceny naruszenia i postępuje zgodnie z rozporządzeniem RODO, ustawą o ochronie danych osobowych oraz wewnętrznymi procedurami Instytucji.

	W przypadku zgłoszeń incydentów przesyłanych w SD przez Administratorów Merytorycznych Instytucji niższego poziomu: W przypadku przekazania na poziom IZ w SD zgłoszenia podatności, zdarzenia lub incydentu przez AM I, przesyła zgłoszenie na poziom IK.
Administrator Merytoryczny w IK	**W przypadku zgłoszeń podatności, zdarzeń lub incydentów otrzymanych od Użytkowników z IK:** a) Otrzymuje od Użytkownika pocztą elektroniczną (następnie je archiwizuje) zgłoszenie dot. podatności, zdarzenia lub incydentu, b) Weryfikuje poprawność typu zgłoszenia. Jeśli nie jest to zgłoszenie dotyczące bezpieczeństwa informacji, to zmienia typ zgłoszenia na właściwy i postępuje zgodnie z procedurami opisanymi w punkcie punktach 3.2, c) Jeśli jest to zgłoszenie dot. bezpieczeństwa informacji, to AM IK powinien: • Potwierdzić, czy zagrożenie bezpieczeństwa rzeczywiście miało miejsce i czy zostało właściwie zakwalifikowane przez zgłaszającego jako podatność, zdarzenie lub incydent, • Ustalić, czy istnieje zagrożenie dla funkcjonowania Systemu, • Ustalić, czy komputer powinien zostać odizolowany od sieci; jeśli tak, to poinformować o tym służby informatyczne Instytucji, • Zabezpieczyć dowody zdarzenia, • Zalecić Użytkownikowi sposób dalszego postępowania lub, jeśli podejrzenie naruszenia bezpieczeństwa nie zostało potwierdzone, poinformować go o możliwości kontynuowania pracy. d) Rejestruje podatność, zdarzenie lub incydent w SD. W przypadku braku dostępności SD AM IK dokonuje zgłoszenia pocztą elektroniczną na adres cst@mfipr.gov.pl . Zgłoszenie dotyczące incydentu należy oznaczy w tytule wiadomości, w nawiasie kwadratowym słowem „[INCYDENT]”. e) Informuje Użytkownika o zamknięciu zgłoszenia – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości), f) Sporządza notatkę o zagrożeniu, jeśli zostanie o to poproszony przez ABI oraz stosuje się do zaleceń wydanych przez ABI.
	W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych Instytucji niższego poziomu: W przypadku przekazania na poziom IK w SD zgłoszenia podatności, zdarzenia lub incydentu przez AM IZ, przesyła zgłoszenie na poziom ABI.
Administrator Bezpieczeństwa CST/CST2021 (ABI)	Po otrzymaniu zgłoszenia, ABI powinien:

	a) Uzyskać od zgłaszającego oraz w razie potrzeby od Wykonawcy, szczegółowe informacje dotyczące m.in. czasu wystąpienia, opisu okoliczności zdarzenia, b) Ustalić, czy zagrożenie bezpieczeństwa rzeczywiście miało miejsce i czy zostało właściwie zakwalifikowane przez zgłaszającego jako podatność, zdarzenie lub incydent dotyczącego bezpieczeństwa informacji lub przetwarzania danych osobowych. W przypadku potwierdzenia wystąpienia podatność, zdarzenie lub incydent dotyczącego bezpieczeństwa – powiadomić Pełnomocnika ds. SZBI dla CST/CST2021 c) Zalecić właściwemu AM oraz w razie potrzeby także Wykonawcy, sposób dalszego postępowania, d) Wyznaczyć AM oraz, jeśli to konieczne, Wykonawcy termin sporządzenia notatki służbowej o incydencie, e) Powiadomić Gestora Systemu o zaistniałym incydencie, f) Sporządzić Raport z obsługi podatności, zdarzenia lub incydentu. Raport powinien zawierać opis wpływu incydentu na infrastrukturę systemu informatycznego, na stan zbiorów informacji oraz ocenę możliwych negatywnych przyszłych skutków incydentu. Raport z obsługi podatności, zdarzenia lub incydentu - jeśli to możliwe - powinien zawierać opinię czy incydent był przypadkowy, czy spowodowany celowo, g) Przy sporządzaniu Raportu z obsługi podatności, zdarzenia lub incydentu ABI może zwrócić się do Wykonawcy lub właściwej Instytucji o dodatkowe informacje, h) Raport powinien zawierać, w formie wniosków końcowych, zalecenia mające na celu podniesienie poziomu bezpieczeństwa oraz ograniczanie skutków incydentów w przyszłości, i) Obsłużyć zgłoszenie dotyczące zagrożenia bezpieczeństwa Systemu w SD i je zamknąć, j) W przypadku podatności, zdarzenia lub incydentu związanego z przetwarzaniem danych osobowych – informuje IOD w Ministerstwie o wystąpieniu naruszenia ochrony danych osobowych i postępach w sprawie, k) Przekazać informację do BPB w Ministerstwie o odnotowanych zdarzeniach, podatnościach, incydentach.
IOD w Ministerstwie	a) Otrzymuje informację od ABI o zgłoszeniu dotyczącym podatności, zdarzenia lub incydentu związanego z przetwarzaniem danych osobowych, b) Po zakończeniu obsługi zgłoszenia przez ABI otrzymuje Raport z obsługi podatności, zdarzenia lub incydentu związanego z przetwarzaniem danych osobowych w CST/CST2021.
Wykonawca	a) Podejmuje zgłoszenie przekazane przez Administratora Bezpieczeństwa CST/ CST2021 (ABI) lub Administratora Merytoryczny IK. b) Podejmuje działania naprawcze w celu wyeliminowania zgłoszonego problemu, c) W przypadku wystąpienia przez ABI - przekazuje ABI wszystkie informacje związane z obsługą zgłoszenia, oraz dane niezbędne do sporządzenia Raportu z obsługi. d) Informuje ABI o sposobie naprawienia błędu.

e)

3.3.2 Ścieżka przepływu zgłoszeń dotyczących zagrożenia bezpieczeństwa informacji

Użytkownik obsługiwany przez IOI/IOR ↔ Administrator Merytoryczny w Instytucji ↔Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny IK↔ABI ↔Wykonawca

Użytkownik obsługiwany przez AM I↔ Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny w IK↔ABI↔Wykonawca

Użytkownik obsługiwany przez AM IZ↔ Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny w IK↔ABI↔Wykonawca

Użytkownik obsługiwany przez AM IK↔ Administrator Merytoryczny w IK↔ABI↔Wykonawca

3.3.3 Ścieżka przepływu zgłoszeń dotyczących naruszenia (bezpieczeństwa) ochrony danych osobowych

Użytkownik obsługiwany przez IOI/IOR ↔ Administrator Merytoryczny w Instytucji ↔Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny IK↔ABI ↔Wykonawca↔IOD MFiPR

Użytkownik obsługiwany przez AM I ↔ Administrator Merytoryczny w Instytucji ↔Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny IK ↔ABI↔Wykonawca↔IOD MFiPR

Użytkownik obsługiwany przez AM IZ↔ Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny w IK ↔ABI↔Wykonawca↔IOD MFiPR

Użytkownik obsługiwany przez AM IK↔ Administrator Merytoryczny w IK ↔ABI↔Wykonawca↔IOD MFiPR

3.3.4 Ocena poziomu priorytetu incydentu bezpieczeństwa lub incydentu związanego z przetwarzaniem danych osobowych

Administrator Bezpieczeństwa CST/CST2021 (ABI) ocenia poziom priorytetu incydentu pod względem dwóch aspektów: wpływu incydentu na organizację oraz pilności znalezienia rozwiązania.

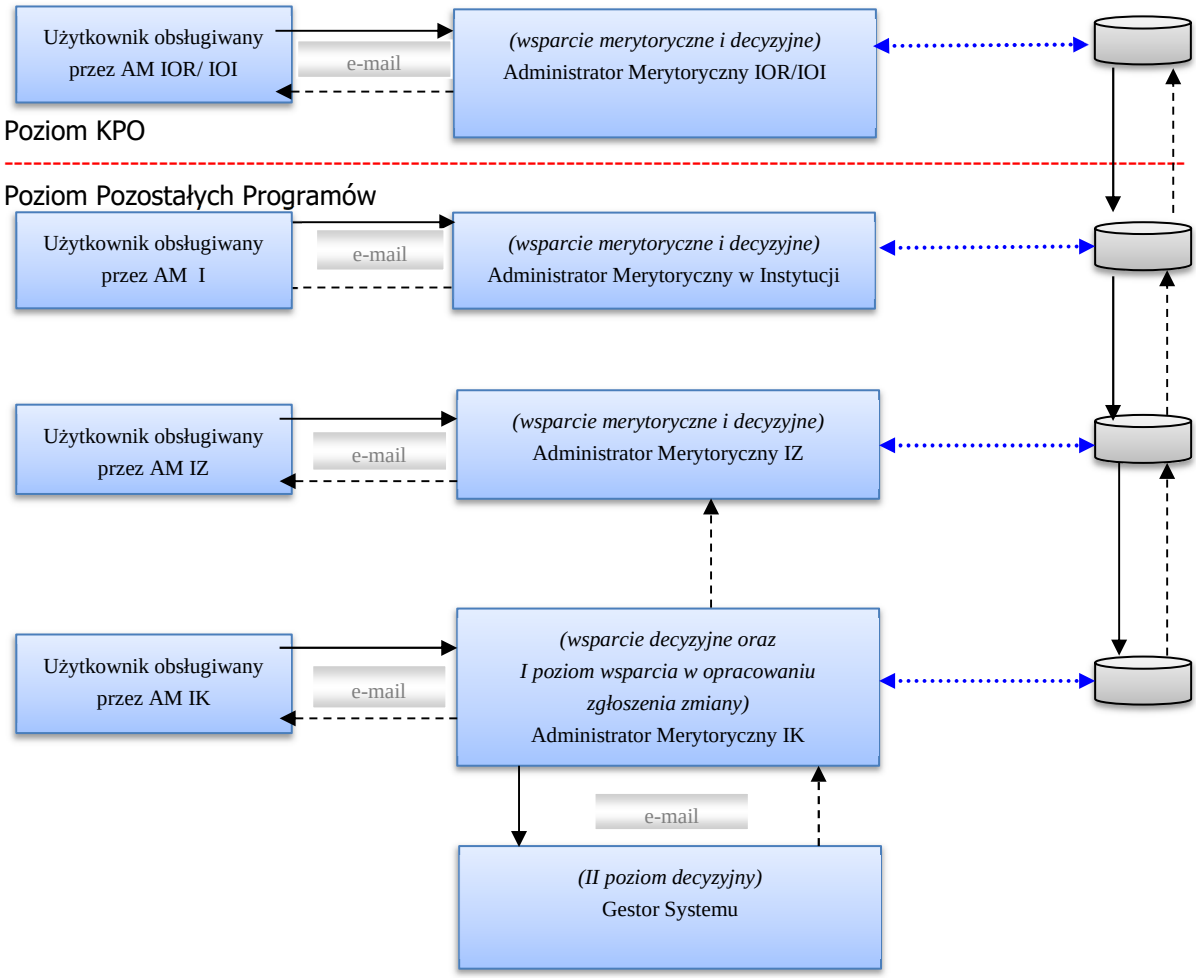
Poziom priorytetu	Wpływ incydentu na organizację	Niezwłoczność podjęcia działań naprawczych
Drobny	Brak wpływu na organizację	Incydent bezpieczeństwa lub incydent związany z przetwarzaniem danych osobowych nie wymaga podejmowania pilnych działań naprawczych
Znaczący	Niski wpływ na organizację	Incydent bezpieczeństwa lub incydent związany z przetwarzaniem danych osobowych wymaga podjęcia działań, których stopień pilności określa organizacja

Krytyczny	Średni wpływ na organizację	Incydent bezpieczeństwa lub incydent związany z przetwarzaniem danych osobowych wymaga podjęcia niezwłocznych działań naprawczych
Blokujący	Wysoki wpływ na organizację	Incydent bezpieczeństwa lub incydent związany z przetwarzaniem danych osobowych wymaga natychmiastowego podjęcia działań naprawczych

3.4 Zgłoszenie potrzeby zmiany Systemu

3.4.1 Diagram procedury

Baza Wiedzy o Funduszach Europejskich, Biblioteka CST2021, SD-*podstawowy poziom wsparcia merytorycznego.*
Użytkownik/Administrator powinien przed zgłoszeniem problemu zapoznać się z informacjami zamieszczonymi w Bazie wiedzy, Bibliotece CST2021 (instrukcjach użytkownika, materiałach dodatkowych) oraz podobnych zgłoszeniach w SD.



3.4.2 Role i zadania

Role	***Zadania***
Użytkownik	W przypadku stwierdzenia potrzeby zmiany w funkcjonowaniu Systemu, Użytkownik sporządza opis zmiany i przesyła go pocztą elektroniczną do właściwego Administratora Merytorycznego.
Administrator Merytoryczny w IOR/IOI	a) Otrzymuje pocztą elektroniczną zgłoszenie (następnie je archiwizuje) zgłoszenie dot. zmiany w postaci opisowej. b) Przeprowadza analizę zgłoszenia zmiany i jeśli zgłoszenie zmiany jest zasadne – rejestruje zgłoszenie zmiany w SD, c) Jeśli to konieczne, dołącza w SD do zgłoszenia zmian załączniki i szczegółowy opis zmiany oraz podaje przyczynę przekazania, a następnie przekazuje zgłoszenie na poziom Administratora Merytorycznego Instytucji, d) W uzasadnionych przypadkach, po analizie zgłoszenia zmiany, może odrzucić zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie zmienia wtedy status na Zamknięte), e) Weryfikuje sposób realizacji zgłoszenia zmiany na wyższych poziomach wsparcia, zamyka zgłoszenie lub przekazuje je do ponownej realizacji w przypadku reklamacji, f) Informuje Użytkownika o zamknięciu zgłoszenia zmiany - przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości). Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „IOR_IOI_Zamknięte" IOR IOI tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie" IOR_IOI_Zamknięte".
Administrator Merytoryczny w Instytucji	Otrzymuje pocztą elektroniczną (następnie je archiwizuje) zgłoszenie dot. zmiany w postaci opisowej. a) przeprowadza analizę zgłoszenia zmiany i jeżeli zgłoszenie jest zasadne – rejestruje zgłoszenie zmiany w SD, b) jeśli to konieczne, dołącza w SD do zgłoszenia zmiany załączniki i szczegółowy opis zmiany oraz podaje przyczynę przekazania, a następnie przekazuje zgłoszenie na poziom Administratora Merytorycznego w IZ, c) w uzasadnionych przypadkach, po analizie zgłoszenia zmiany, może odrzucić zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie zmiany zmienia wtedy status na Zamknięte), d) weryfikuje sposób realizacji zgłoszenia zmiany na wyższych poziomach wsparcia, zamyka zgłoszenie lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, e) informuje Użytkownika o zamknięciu zgłoszenia zmiany – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości). Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „AMI_Zamknięte" AMI tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie "AMI_zamknięte".
Administrator Merytoryczny w IZ	**W przypadku zgłoszeń otrzymanych od Użytkowników z IZ:** Otrzymuje pocztą elektroniczną (następnie je archiwizuje) zgłoszenie dot. zmiany w postaci opisowej. a) przeprowadza analizę zgłoszenia zmiany i jeżeli zgłoszenie zmiany jest zasadne – rejestruje zgłoszenie zmiany w SD, b) jeśli to konieczne, dołącza do zgłoszenia załączniki i szczegółowy opis zmiany

Role	***Zadania***
	oraz podaje przyczynę przekazania, a następnie przekazuje zgłoszenie na poziom Administratora Merytorycznego w IZ, c) w uzasadnionych przypadkach, po analizie zgłoszenia zmiany, może odrzucić zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie zmiany zmienia wtedy status na zamknięte), d) weryfikuje sposób realizacji zgłoszenia zmiany na wyższych poziomach wsparcia, zamyka zgłoszenie lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, e) informuje Użytkownika o zamknięciu zgłoszenia zmiany – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości). **W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych Instytucji niższego poziomu:** a) przeprowadza analizę zgłoszenia zmiany i jeżeli zgłoszenie zmiany jest zasadne – przesyła je w SD na poziom AM IK, b) jeśli zgłoszenie zmiany nie jest zasadne to może je odrzucić, podając przy tym przyczynę odrzucenia, c) jeśli zgłoszenie zmiany wymaga uzupełnienia to może cofnąć zgłoszenie do AMI, d) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, e) przekazuje zgłoszenia do weryfikacji na poziomie AMI. Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „AM IZ_Zamknięte" AMI tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie "AM IZ_zamknięte".
Administrator Merytoryczny w IK	**W przypadku zgłoszeń otrzymanych od Użytkowników z IK:** Otrzymuje pocztą elektroniczną (następnie je archiwizuje) zgłoszenie dot. zmiany w postaci opisowej. a) przeprowadza analizę zgłoszenia zmiany i jeżeli zgłoszenie zmiany jest zasadne, rejestruje zgłoszenie zmiany w SD, b) jeśli to konieczne, dołącza w SD do zgłoszenia zmiany załączniki i szczegółowy opis zmiany, c) w uzasadnionych przypadkach, po analizie zgłoszenia, może odrzucić zgłoszenie w SD podając przy tym przyczynę odrzucenia (zgłoszenie zmiany zmienia wtedy status na zamknięte), d) w uzasadnionych przypadkach, po analizie zgłoszenia, może zamrozić zgłoszenie w celu jego późniejszej realizacji, e) weryfikuje sposób realizacji zgłoszenia, f) zamyka zgłoszenia po zakończeniu jego realizacji lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, g) informuje Użytkownika o zamknięciu zgłoszenia zmiany – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości). Uwaga: AM IK może ponownie otworzyć zgłoszenie zmiany, które posiada status „IK_Zamknięte". **W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych Instytucji niższego poziomu:** a) przeprowadza analizę zgłoszenia zmiany i jeżeli zgłoszenie zmiany jest zasadne, wpisuje propozycję zmiany do rejestru zmian, b) jeśli zgłoszenie zmiany nie jest zasadne - odrzuca je, podając przy tym przyczynę odrzucenia,

Role	***Zadania***
	c) w uzasadnionych przypadkach, po analizie zgłoszenia, może zamrozić zgłoszenie w celu jego późniejszej realizacji. d) jeśli zgłoszenie zmiany wymaga uzupełnienia - cofa zgłoszenie do AM IZ, e) zamyka zgłoszenie lub przekazuje je do ponownej realizacji w przypadku jego reklamacji. Uwaga: AM IK może otworzyć zgłoszenie zmiany, które posiada status „IK_Zamknięte”.
Gestor Systemu	Po otrzymaniu za pośrednictwem poczty elektronicznej propozycji zmiany w Systemie, Gestor Systemu: a) wyraża zgodę na wprowadzenie proponowanej zmiany w Systemie, b) w uzasadnionych przypadkach nie wyraża zgody na wprowadzenie zmiany lub zamraża zmianę - do realizacji w późniejszym okresie, c) zgłasza uwagi do zaproponowanej zmiany w Systemie

3.4.3 Ścieżka przepływu zgłoszeń zmiany Systemu

Użytkownik obsługiwany przez AM / IOR / IOI→ Administrator Merytoryczny w IOR IOI→ Administrator Merytoryczny w Instytucji →Administrator Merytoryczny w IZ → Administrator Merytoryczny IK

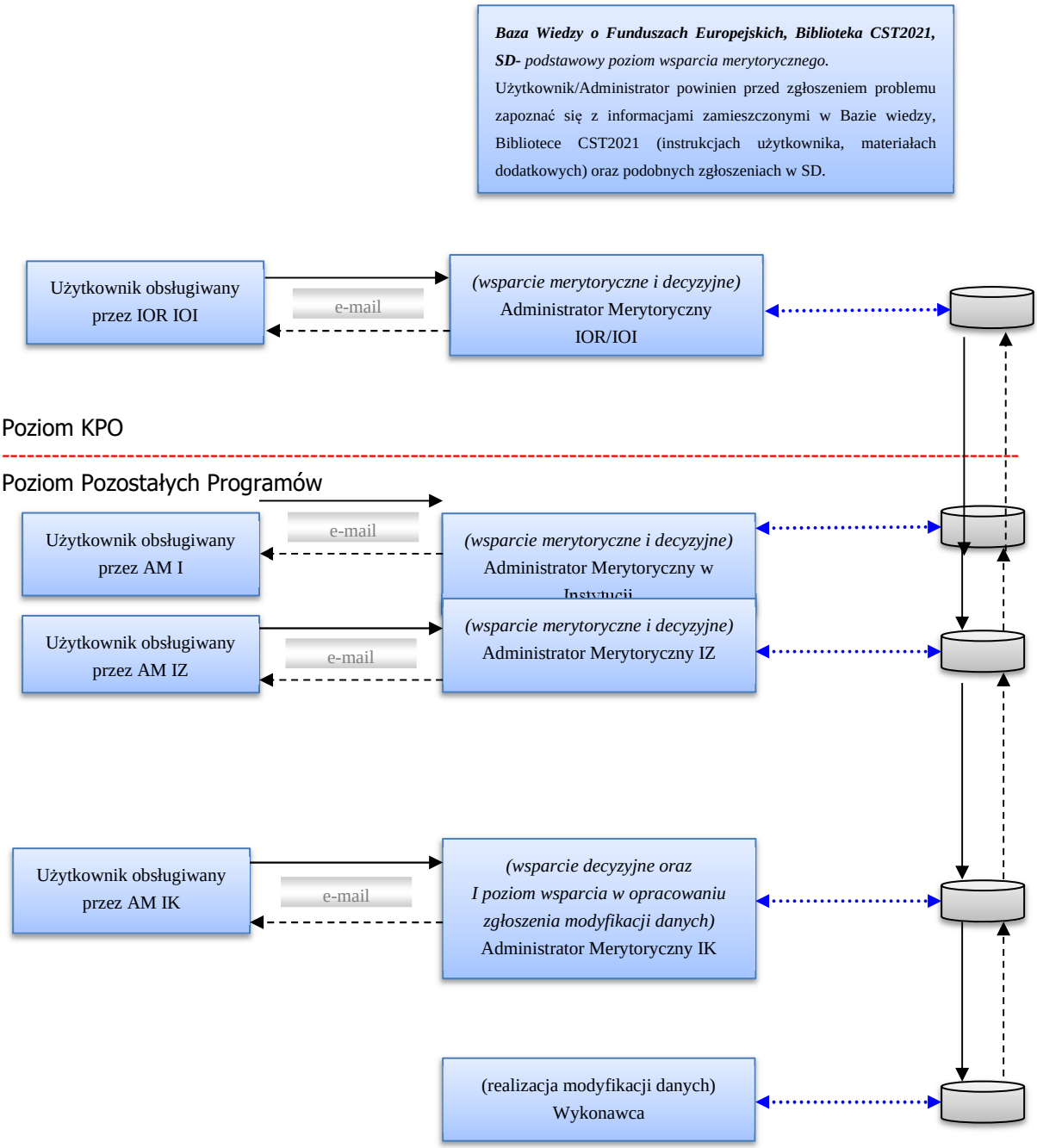
Użytkownik obsługiwany przez AM I→ Administrator Merytoryczny w Instytucji →Administrator Merytoryczny w IZ → Administrator Merytoryczny IK.

Użytkownik obsługiwany przez AM IZ→ Administrator Merytoryczny w IZ → Administrator Merytoryczny w IK.

Użytkownik obsługiwany przez AM IK→ Administrator Merytoryczny w IK.

3.5 Zgłoszenie potrzeby modyfikacji danych w Systemie (skrypt porządkujący dane)

3.5.1 Diagram procedury



3.5.2 Role i zadania

Role	***Zadania***
Użytkownik	W przypadku stwierdzenia potrzeby modyfikacji danych w Systemie, Użytkownik sporządza jej opis i przesyła pocztą elektroniczną do właściwego Administratora Merytorycznego.
Administrator Merytoryczny w IOR/ IOI	Otrzymuje zgłoszenie dot. modyfikacji danych w postaci opisowej (archiwizuje zgłoszenie). a) przeprowadza analizę zgłoszenia modyfikacji danych i jeżeli zgłoszenie jest zasadne, rejestruje zgłoszenie w SD; b) jeśli to konieczne, dołącza w SD do zgłoszenia modyfikacji danych załączniki i szczegółowy opis modyfikacji, podaje przyczynę przekazania, a następnie przekazuje zgłoszenie na poziom Administratora Merytorycznego w I; c) w uzasadnionych przypadkach, po analizie zgłoszenia modyfikacji danych, może odrzucić zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie modyfikacji danych zmienia wtedy status na zamknięte); d) weryfikuje sposób realizacji zgłoszenia zmiany na wyższych poziomach wsparcia, zamyka zgłoszenie lub przekazuje je do ponownej realizacji w przypadku jego reklamacji; e) informuje Użytkownika o zamknięciu zgłoszenia modyfikacji danych – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości).
Administrator Merytoryczny w Instytucji	Otrzymuje zgłoszenie dot. modyfikacji danych w postaci opisowej (archiwizuje zgłoszenie). a) przeprowadza analizę zgłoszenia modyfikacji danych i jeżeli zgłoszenie jest zasadne – rejestruje zgłoszenie w SD; b) jeśli to konieczne, dołącza w SD do zgłoszenia modyfikacji danych załączniki i szczegółowy opis modyfikacji, podaje przyczynę przekazania, a następnie przekazuje zgłoszenie na poziom Administratora Merytorycznego w IZ; c) w uzasadnionych przypadkach, po analizie zgłoszenia modyfikacji danych, może odrzucić zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie modyfikacji danych zmienia wtedy status na zamknięte); d) weryfikuje sposób realizacji zgłoszenia zmiany na wyższych poziomach wsparcia, zamyka zgłoszenie lub przekazuje je do ponownej realizacji w przypadku jego reklamacji; e) informuje Użytkownika o zamknięciu zgłoszenia modyfikacji danych – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości).
	W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych IOR/IOI niższego poziomu: a) przeprowadza analizę zgłoszenia modyfikacji danych i jeżeli zgłoszenie jest zasadne, przesyła je w SD na poziom IZ, b) jeśli zgłoszenie modyfikacji danych nie jest zasadne to może je odrzucić, podając przy tym przyczynę odrzucenia, c) jeśli zgłoszenie modyfikacji danych wymaga uzupełnienia to może cofnąć zgłoszenie do AM IOR/ IOI, d) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, e) przekazuje zgłoszenia do weryfikacji na poziomie IOR IOI.

Role	***Zadania***
	Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „AM I_Zamknięte" AM I tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie "AM I_zamknięte".
Administrator Merytoryczny w IZ	**W przypadku zgłoszeń otrzymanych od Użytkowników z IZ:** Otrzymuje od Użytkownika pocztą elektroniczną (następnie je archiwizuje) zgłoszenie dot. modyfikacji danych w postaci opisowej. a) przeprowadza analizę zgłoszenia zmiany i jeżeli zgłoszenie zmiany jest zasadne – rejestruje zgłoszenie zmiany w SD; b) jeśli to konieczne, dołącza w SD do zgłoszenia załączniki i szczegółowy opis modyfikacji danych oraz podaje przyczynę przekazania, a następnie przekazuje zgłoszenie na poziom Administratora Merytorycznego w IK, c) w uzasadnionych przypadkach, po analizie zgłoszenia zmiany, może odrzucić zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie zmiany zmienia wtedy status na zamknięte), d) weryfikuje sposób realizacji zgłoszenia zmiany na wyższych poziomach wsparcia, zamyka zgłoszenie lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, e) informuje Użytkownika o zamknięciu zgłoszenia modyfikacji danych – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości).
	W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych Instytucji niższego poziomu: a) przeprowadza analizę zgłoszenia modyfikacji danych i jeżeli zgłoszenie jest zasadne, przesyła je w SD na poziom IK, b) jeśli zgłoszenie modyfikacji danych nie jest zasadne to może je odrzucić, podając przy tym przyczynę odrzucenia, c) jeśli zgłoszenie modyfikacji danych wymaga uzupełnienia to może cofnąć zgłoszenie do AMI, d) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, e) przekazuje zgłoszenia do weryfikacji na poziomie AMI. Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „AM IZ_Zamknięte" AM IZ tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie "AM IZ_zamknięte".

Role	***Zadania***
Administrator Merytoryczny w IK	**W przypadku zgłoszeń otrzymanych od Użytkowników z IK:** Otrzymuje od Użytkownika pocztą elektroniczną (następnie je archiwizuje) zgłoszenie dot. modyfikacji danych w postaci opisowej. a) przeprowadza analizę zgłoszenia i jeżeli jest ono zasadne, rejestruje je w SD; b) jeśli to konieczne, dołącza w SD do zgłoszenia załączniki i szczegółowy opis modyfikacji danych, c) w uzasadnionych przypadkach, po analizie zgłoszenia, może odrzucić zgłoszenie w SD podając przy tym przyczynę odrzucenia (zgłoszenie modyfikacji danych zmienia wtedy status na zamknięte), d) w uzasadnionych przypadkach, po analizie zgłoszenia, może zamrozić zgłoszenie w celu jego późniejszej realizacji, e) przekazuje zgłoszenie do Wykonawcy, podając przy tym przyczynę przekazania, f) weryfikuje sposób realizacji zgłoszenia na poziomie Wykonawcy lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, g) informuje Użytkownika o zamknięciu zgłoszenia modyfikacji danych – przesyła do niego odpowiedź pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości). Uwaga: AM IK może ponownie otworzyć zgłoszenie modyfikacji danych, które posiada status „IK_Zamknięte”.
	W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych niższego poziomu: a) przeprowadza analizę zgłoszenia modyfikacji danych i jeżeli zgłoszenie jest zasadne – przesyła je do Wykonawcy, b) jeśli zgłoszenie nie jest zasadne to może je odrzucić, podając przy tym przyczynę odrzucenia, c) w uzasadnionych przypadkach, po analizie zgłoszenia, może zamrozić zgłoszenie w celu jego późniejszej realizacji, d) jeśli zgłoszenie wymaga uzupełnienia to może cofnąć zgłoszenie do AM IZ, e) weryfikuje sposób realizacji zgłoszenia na poziomie Wykonawcy lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, f) przekazuje zgłoszenia do weryfikacji na poziomie AM IZ. Uwaga: AM IK może ponownie otworzyć zgłoszenie zmiany, które posiada status „IK_Zamknięte”.
Wykonawca	Obsługuje zgłoszenie dot. modyfikacji danych w SD: a) realizuje zgłoszenie: Wykonawca zobowiązany jest uzupełnić:

Role	***Zadania***
	– wpis w polu audytowym Systemu „Kto modyfikował” wpisem „XXXXXX - Skrypt porządkujący dane” (gdzie „X” oznacza numer zgłoszenia w SD), – wpis w polu audytowym Systemu „Kiedy modyfikował” datą wykonania skryptu, – analogiczne wpisy w tabeli Systemu przechowującej historię pól tabel. Wykonawca zobowiązany jest także do przetestowania skryptu porządkującego dane przed uruchomieniem go na bazie produkcyjnej. b) proponuje odrzucenie zgłoszenia w SD, podając przy tym przyczynę odrzucenia, c) cofa zgłoszenie na niższy poziom w celu jego uzupełnienia.

3.5.3 Ścieżka przepływu zgłoszeń

Użytkownik obsługiwany przez IOR / IOI↔ Administrator Merytoryczny w IOR IOI↔Administrator Merytoryczny w Instytucji ↔ Administrator Merytoryczny IZ↔ Administrator Merytoryczny w IK↔Wykonawca

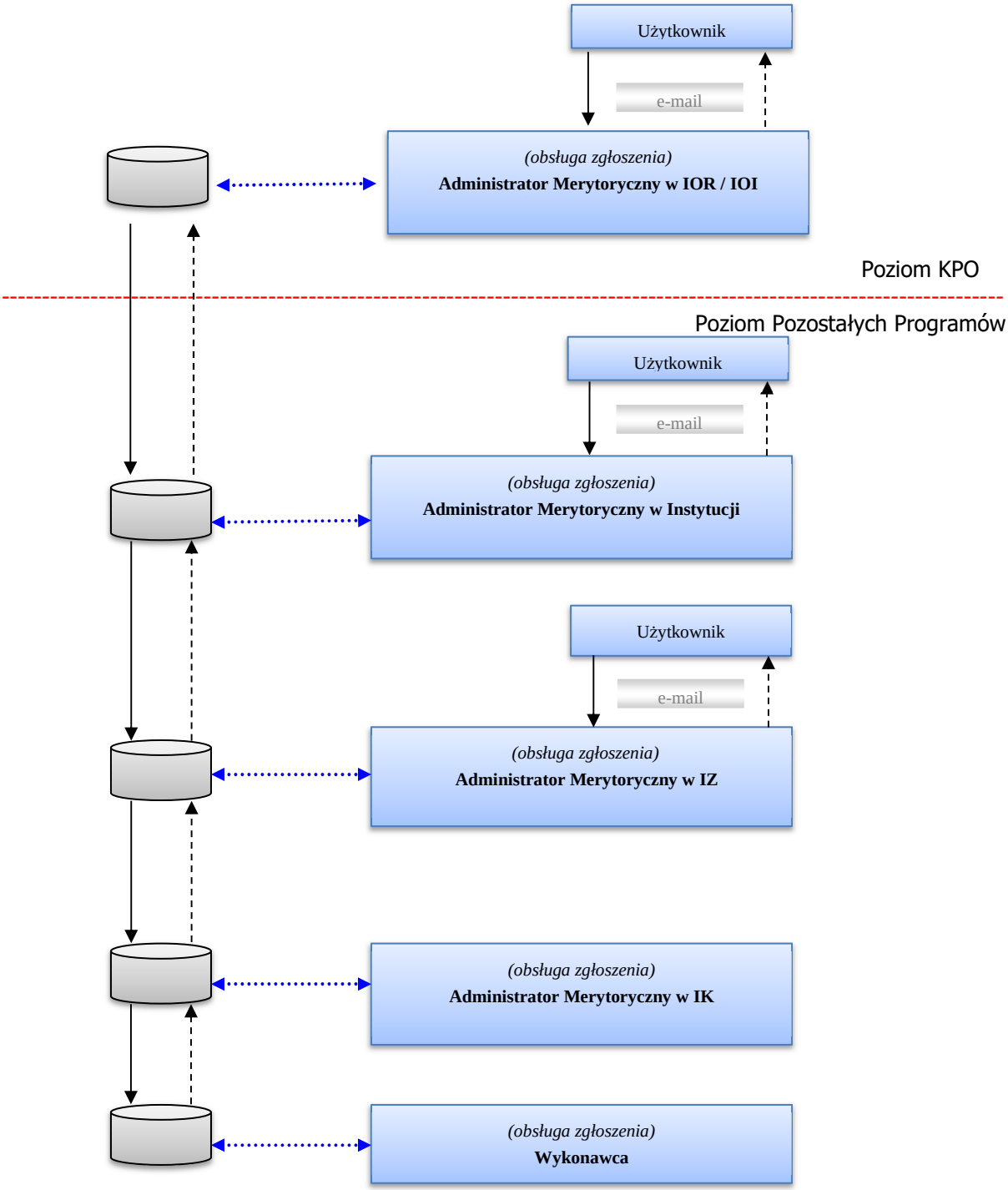
Użytkownik obsługiwany przez AM I↔ Administrator Merytoryczny w Instytucji ↔Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny IK↔ ↔Wykonawca.

Użytkownik obsługiwany przez AM IZ↔ Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny w IK↔Wykonawca.

Użytkownik obsługiwany przez AM IK↔ Administrator Merytoryczny w IK↔Wykonawca.

3.6 Obsługa zgłoszeń dot. problemu braku możliwości terminowego przedłożenia danych w Systemie

3.6.1 Diagram procedury



3.6.2 Role i zadania

Rola	*Zadania*
Użytkownik	W przypadku braku możliwości terminowego przedłożenia danych w Systemie spowodowanego błędem lub awarią, Użytkownik informuje o fakcie odpowiedniego Administratora Merytorycznego za pośrednictwem poczty elektronicznej.
Administrator Merytoryczny w IOR/IOI	W przypadku otrzymania za pośrednictwem poczty elektronicznej (potrzeba archiwizacji) zgłoszenia o braku możliwości terminowego przedłożenia danych w Systemie, spowodowanego błędem lub awarią Systemu Administrator Merytoryczny IOR / IOI: a) Opracowuje zgłoszenie problemu poprzez wypełnienie załącznika nr 3 do niniejszego dokumentu, b) Przeprowadza analizę zgłoszenia- sprawdza w bazie zgłoszeń SD czy podobne zgłoszenie nie było już obsługiwane, c) Jeśli może sam udzielić właściwej odpowiedzi, przesyła ją Użytkownikowi za pomocą poczty elektronicznej (sugeruje się archiwizowanie informacji/odpowiedzi przesłanej pocztą elektroniczną), d) Jeżeli zgłoszenie jest zasadne i Administrator IOR / IOI nie może sam udzielić właściwej odpowiedzi, rejestruje zgłoszenie w SD wybierając odpowiedni typ zgłoszenia „UCHYBIENIE TERMINU", e) Dołącza w SD do zgłoszenia „Formularz zgłoszenia problemu rejestracji danych w Systemie" i jeśli to konieczne, bardziej szczegółowy opis problemu, f) W uzasadnionych przypadkach, po analizie zgłoszenia, może odrzucić zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie problemu zmienia wtedy status na zamknięte), g) Jeśli nie potrafi rozwiązać problemu, to przekazuje zgłoszenie na poziom Administratora Merytorycznego w Instytucji, podając przy tym przyczynę przekazania, h) Jeśli potrafi rozwiązać problem samodzielnie, to rozwiązuje problem, przesyła pocztą elektroniczną (wskazana potrzeba archiwizacji) odpowiedź i zamyka zgłoszenie, i) Weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia, zamyka zgłoszenie lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, j) Informuje Użytkownika o zamknięciu zgłoszenia- przesyła do niego pocztą elektroniczną (wskazanie potrzeby archiwizacji). Uwaga: w celu wznowienia prac nad zgłoszenie, które posiada status „IOR_IOI_ZAMKNIĘTE" IORIOI tworzy nowe zgłoszenie, do którego wiąże nowe zgłoszenie o statusie „IOR_IOI_ZAMKNIĘTE".
Administrator Merytoryczny w Instytucji	W przypadku otrzymania za pośrednictwem poczty elektronicznej (potrzeba archiwizacji) zgłoszenia o braku możliwości terminowego przedłożenia danych w Systemie, spowodowanego błędem lub awarią Systemu, AM I: a) opracowuje zgłoszenie problemu poprzez wypełnienie załączniku nr 3 do niniejszego dokumentu, b) przeprowadza analizę zgłoszenia – sprawdza w bazie zgłoszeń SD czy podobne zgłoszenie nie było już obsługiwane, c) jeśli może sam udzielić właściwej odpowiedzi, przesyła ją Użytkownikowi za pomocą poczty elektronicznej (sugeruje się archiwizowanie informacji/ odpowiedzi przesłanej pocztą elektroniczną), d) jeżeli zgłoszenie jest zasadne i AM I nie może sam udzielić właściwej odpowiedzi, rejestruje zgłoszenie w SD wybierając odpowiedni typ zgłoszenia „UCHYBIENIE TERMINU", e) dołącza w SD do zgłoszenia „Formularz zgłoszenia problemu rejestracji danych w Systemie „i jeśli to konieczne, bardziej szczegółowy opis problemu, f) w uzasadnionych przypadkach, po analizie zgłoszenia, może odrzucić

Rola	***Zadania***
	zgłoszenie podając przy tym przyczynę odrzucenia (zgłoszenie problemu zmienia wtedy status na Zamknięte), g) jeśli nie potrafi rozwiązać problemu, to przekazuje zgłoszenie na poziom Administratora Merytorycznego w IZ, podając przy tym przyczynę przekazania, h) jeśli potrafi rozwiązać problem samodzielnie, rozwiązuje problem, przesyła pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości) i zamyka zgłoszenie, i) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia, zamyka zgłoszenie lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, j) informuje Użytkownika o zamknięciu zgłoszenia – przesyła do niego pocztą elektroniczną (wskazana potrzeba archiwizacji wiadomości). Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „AMI_Zamknięte" AMI tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie "AMI_zamknięte". **W przypadku zgłoszeń przesyłanych w SD przez Administratorów Merytorycznych niższego poziomu:** a) przeprowadza analizę zgłoszenia dotyczącego braku możliwości terminowego przedłożenia danych, b) jeśli zgłoszenie nie jest zasadne, może je odrzucić, podając przy tym przyczynę odrzucenia, c) przekazuje zgłoszenie na wyższy poziom do AM IZ, w celu jego realizacji, d) jeśli zgłoszenie wymaga uzupełnienia, może cofnąć zgłoszenie do AM IOR/ IOI, e) weryfikuje sposób realizacji zgłoszenia na poziomie AM IZ, f) przekazuje zgłoszenia do weryfikacji na poziom AM IOR/ IOI.
Administrator Merytoryczny w IZ	W przypadku otrzymania za pośrednictwem poczty elektronicznej (potrzeba archiwizacji) zgłoszenia o braku możliwości terminowego przedłożenia danych w Systemie, spowodowanego błędem lub awarią Systemu lub zgłoszenia od AMI, AM IZ: a) opracowuje zgłoszenie problemu poprzez wypełnienie załącznika nr 3 do niniejszego dokumentu lub przeprowadza analizę zgłoszenia AM I – sprawdza w SD czy podobne zgłoszenie nie było już obsługiwane. W wyniku analizy AM IZ może cofnąć zgłoszenie do AM I, b) jeśli nie może sam udzielić właściwej odpowiedzi, podaje przyczynę przekazania, a następnie przekazuje zgłoszenie na poziom Administratora Merytorycznego w IK, c) jeśli zgłoszenie nie jest zasadne, odrzuca je, podając przyczynę odrzucenia, d) jeśli zgłoszenie wymaga uzupełnienia - cofa zgłoszenie do AM I, e) jeśli potrafi rozwiązać problem samodzielnie, rozwiązuje problem i przekazuje je do weryfikacji na niższym poziomie wsparcia, f) weryfikuje sposób realizacji zgłoszenia na wyższych poziomach wsparcia lub przekazuje je do ponownej realizacji w przypadku jego reklamacji, g) przekazuje zgłoszenie do weryfikacji na poziomie AM I. Uwaga: W celu wznowienia prac nad zgłoszeniem, które posiada status „AM IZ_Zamknięte" AMI tworzy nowe zgłoszenie, do którego wiąże zgłoszenie o statusie "AM IZ_zamknięte".

Rola	*Zadania*
Administrator Merytoryczny w IK	Obsługuje zgłoszenie w SD: a) przeprowadza analizę zgłoszenia – sprawdza w SD czy podobne zgłoszenie nie było już obsługiwane. W wyniku analizy AM IK może cofnąć zgłoszenie do AM IZ, b) analizuje dane dot. przyczyn braku możliwości przedłożenia dokumentu w Systemie, c) jeśli nie może sam udzielić właściwej odpowiedzi, podaje przyczynę przekazania, a następnie przesyła zgłoszenie do Wykonawcy, d) jeśli zgłoszenie nie jest zasadne, może je odrzucić, e) jeśli zgłoszenie wymaga uzupełnienia, cofa zgłoszenie do AM IZ, f) jeśli potrafi rozwiązać problem samodzielnie, rozwiązuje problem i przekazuje je do weryfikacji na niższym poziomie wsparcia, g) weryfikuje sposób realizacji zgłoszenia na poziomie Wykonawcy lub przekazuje je do ponownej realizacji w przypadku jego reklamacji bądź uzupełnienia informacji niezbędnych do obsługi zgłoszenia, h) przekazuje zgłoszenie do weryfikacji na poziomie AM IZ.
Wykonawca	Obsługuje zgłoszenie w SD przekazane przez AM IK: a) realizuje zgłoszenie, b) wypełnia i załącza do zgłoszenia raport, w którym potwierdza czy zgłoszenie jest zasadne; Raport zawiera min.: – Nazwę beneficjenta, – Numer umowy, – Numer dokumentu objętego zgłoszeniem (jeśli dotyczy), – Datę zdarzenia, – Krótkie uzasadnienie uznania zgłoszenia za zasadne/odrzucenia. c) przekazuje informacje o Infrastrukturze Systemu, wskazuje elementy, które powodują błąd oraz wszelkie informacji o Systemach potrzebnych do przywrócenia ich pełnej funkcjonalności, d) cofa zgłoszenie na niższy poziom w celu jego uzupełnienia.

3.6.3 Ścieżka przepływu zgłoszeń

Użytkownik obsługiwany przez IOR / IOI↔ Administrator Merytoryczny w IOR IOI↔Administrator Merytoryczny w I ↔ Administrator Merytoryczny IZ ↔ Administrator Merytoryczny IK ↔Wykonawca

Użytkownik obsługiwany przez AM I↔ Administrator Merytoryczny w Instytucji ↔Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny IK ↔Wykonawca.

Użytkownik obsługiwany przez AM IZ↔Administrator Merytoryczny w IZ ↔ Administrator Merytoryczny IK ↔Wykonawca

4. Postępowanie w razie awarii SD

W razie niedostępności SD, zgłaszanie problemu merytorycznego/ obsługowego/ technicznego/ zmiany/ podatności, zdarzenia, incydentu związanego z bezpieczeństwem informacji lub przetwarzaniem danych osobowych, odbywa się za pośrednictwem poczty elektronicznej. Użytkownik przesyła zgłoszenie do AM instytucji, w której pracuje lub instytucji udzielającej wsparcie.

W przypadku braku Administratora Merytorycznego w danej Instytucji, Użytkownik przesyła zgłoszenie do Administratora Merytorycznego Instytucji nadrzędnej, np. Użytkownik IW =>AM w IP, albo Użytkownik IP => AM IZ.
Adres AM IK:
cst@mfipr.gov.pl (do zgłaszania problemów oraz incydentów). Zgłoszenie dotyczące incydentu należy oznaczy w tytule wiadomości, w nawiasie kwadratowym słowem [INCYDENT].

cst.uprawnienia@mfipr.gov.pl (do zgłaszania problemów związanych z uprawnieniami użytkowników).

W razie niedostępności SD proces obsługi zgłoszeń eskalowanych (tj., zgłoszeń których obsługa wymaga prac po stronie Wykonawcy odbywa się również za pośrednictwem poczty elektronicznej w sposób określony w umowie wiążącej Ministerstwo i Wykonawcę.

5. Baza Wiedzy o Funduszach Europejskich, Biblioteka CST2021 oraz SD

Baza Wiedzy o Funduszach Europejskich, Biblioteka CST2021 oraz SD stanową podstawowy poziom wsparcia merytorycznego/ obsługowego/ technicznego. Użytkownik przed zgłoszeniem problemu/ zmiany musi zapoznać się z informacjami zamieszczonymi w wymienionych bazach, w kontekście obszaru, którego dotyczy problem. Podobnie, każdy Administrator Merytoryczny lub pracownik opracowujący odpowiedź, powinien również przed udzieleniem odpowiedzi zapoznać się z informacjami zamieszczonymi we wskazanych bazach w kontekście obszaru w jakim Użytkownik zgłosił problem/ zmianę.

6. Załączniki

6.1 Załącznik nr 1. Formularz zgłaszania problemów

FORMULARZ ZGŁASZANIA PROBLEMÓW		
1	Nazwa aplikacji[1]	
2	Opis problemu	
3	Login użytkownika/-ów zgłaszającego/-ych problem	
4.	Numer projektu[2]	
5.	Rodzaj dokumentu[3]	
6.	Nazwa/numer identyfikacyjny dokumentu[4]	
7.	W przypadku komunikatu o błędzie[5]:	
	7.1 Identyfikator błędu[6]	
	7.2 Data i godzina wystąpienia błędu	
	7.3 Kod instancji aplikacji, na której wystąpił błąd[7]	
	7.4 Podstawowe kroki prowadzące do wystąpienia błędu[8]	
8.	Rodzaj i wersja przeglądarki internetowej	
9.	Ewentualne zrzuty ekranu	

[1] Dostępne wartości: zgodne z pkt. 1.1 procedury

[2] Jeżeli dotyczy

[3] Jeżeli dotyczy konkretnego dokumentu w ramach projektu

[4] Jeżeli dotyczy konkretnego dokumentu w ramach projektu

[5] Komunikat z błędem, błąd na stronie, np. „504")

[6] Jeżeli został wyświetlony na stronie

[7] Jeżeli Użytkownik posiada

[8] Wykonywana operacja, bezpośrednio poprzedzająca wystąpienie błędu

6.2 Załącznik nr 2. Formularz modyfikacji danych

Lp.	nazwa dokumentu	numer dokumentu	blok	nazwa pola	modyfikacja		uzasadnienie
	np. deklaracja wydatków, sprawa/ decyzja w ROP	np. Nr deklaracji wydatków, nr sprawy/ decyzji w ROP	np. Wydatki w podziale na oś/działanie/poddziałanie, Karta informacyjna obciążenia	np. wydatki kwalifikowalne	obecna wartość (jest)	wartość, którą należy wprowadzić (powinno być)	np. Poprawa błędu niemożliwego do usunięcia z poziomu użytkownika wprowadzającego dane
1							
2							
3							

6.3 Załącznik nr 3.Formularz zgłoszenia braku możliwości terminowego przedłożenia danych w Systemie

Formularz zgłoszenia braku możliwości terminowego przedłożenia wymaganych danych w Systemie		
1	Numer umowy o dofinansowanie	
2	Nazwa Beneficjenta	
3	Login użytkownika/ów zgłaszającego/ych problem	
4	Numer i rodzaj dokumentu objętego zgłoszeniem (lub inne dane pozwalające zidentyfikować dokument)	
5	Data i godzina upływu terminu na przedłożenie dokumentu w Systemie	
6	Data i godzina (lub okres) wystąpienia problemu, częstotliwość występowania (jednokrotnie, wielokrotnie)	
7	Opis problemu (zawierający opis wszystkich czynności jakie wykonywał użytkownik przed wystąpieniem problemu oraz potwierdzenie, że nie pracował na dwóch oknach przeglądarki w Systemie)	
8	Nazwy załączników potwierdzających problem (zrzuty ekranu, filmy)	