System Obsługi Incydentów DORA

(SOID)

INSTRUKCJA UŻYTKOWNIKA

Metryka dokumentu:

Data publikacji: 22.01.2025
Wersja: 1.0.1

TLP: CLEAR

Spis treści

Instrukcja ma na celu pomoc w wypełnianiu formularza dotyczącego zgłoszenia incydentu poważnego zgodnie z wymogami rozporządzenia DORA (Digital Operational Resilience Act).

1. Podstawowe informacje

Rozporządzenie DORA nakłada na instytucje finansowe obowiązek zarządzania incydentami związanymi z technologiami informacyjno-komunikacyjnymi (ICT) oraz zgłaszania poważnych incydentów do organu nadzoru.

Incydent poważny związany z ICT to incydent o dużym negatywnym wpływie na sieci i systemy informatyczne wspierające krytyczne lub istotne funkcje podmiotu finansowego.

W celu usystematyzowania oraz uporządkowania klasyfikacji incydentów związanych z ICT, Rozporządzenie DORA wycenia zdarzenia na podstawie wpływu na następujące kryteria:

- liczba lub znaczenie klientów oraz kontrahentów finansowych dotkniętych incydentem,
- czas trwania incydentu ICT (w tym czas niedostępności usług),
- zasięg geograficzny w odniesieniu do obszarów dotkniętych incydentem, w szczególności, jeżeli dotyczy on więcej niż dwóch państw członkowskich,
- utrata danych (dostępności, autentyczności, integralności lub poufności danych),
- krytyczność usług, których dotyczy incydent związany z ICT, w tym transakcji i operacji podmiotu finansowego,
- skutki gospodarcze incydentu związanego z ICT, w szczególności bezpośrednie i pośrednie koszty i strat.

W celu zapewnienia skutecznego przepływu informacji raportowanie incydentów zostało podzielone na 3 etapy:

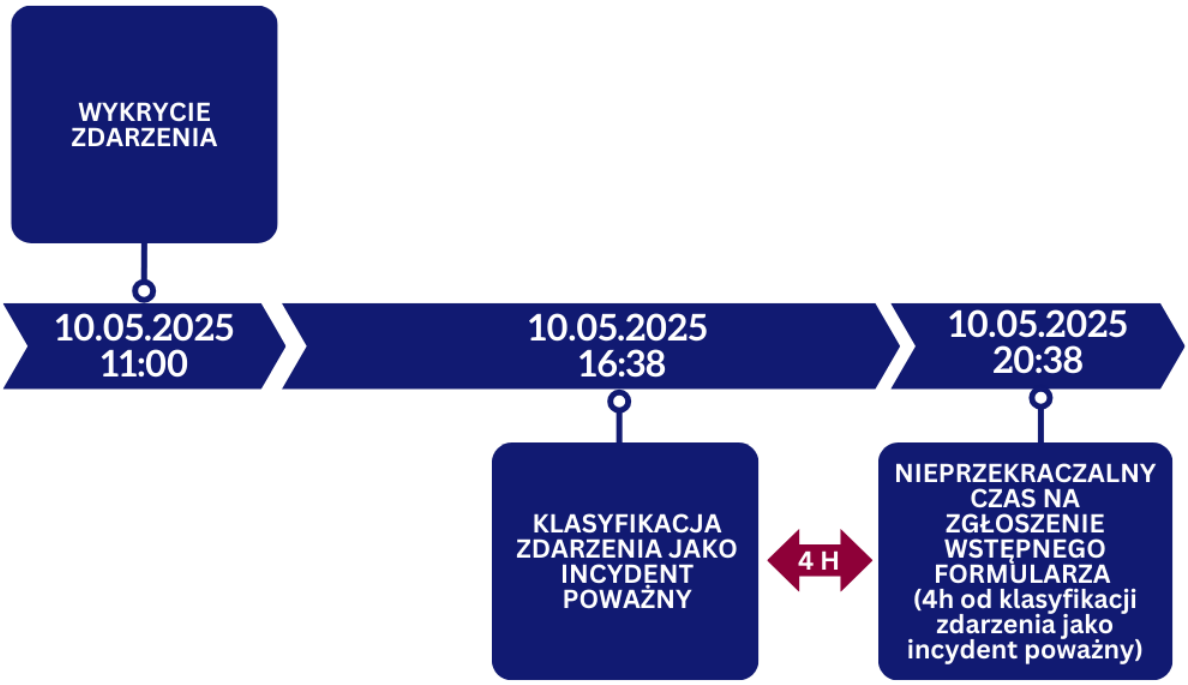
- wstępne powiadomienie;
- sprawozdanie śródokresowe;
- sprawozdanie końcowe.

Dodatkowo zostały także wprowadzone ramy czasowe, na każdy z wyżej wymienionych etapów:

1. Wstępne powiadomienie składane jest:
    a. do **4h** od zaklasyfikowania zdarzenia jako incydent,
    b. ale nie później niż **24 godzin** od wykrycia incydentu.

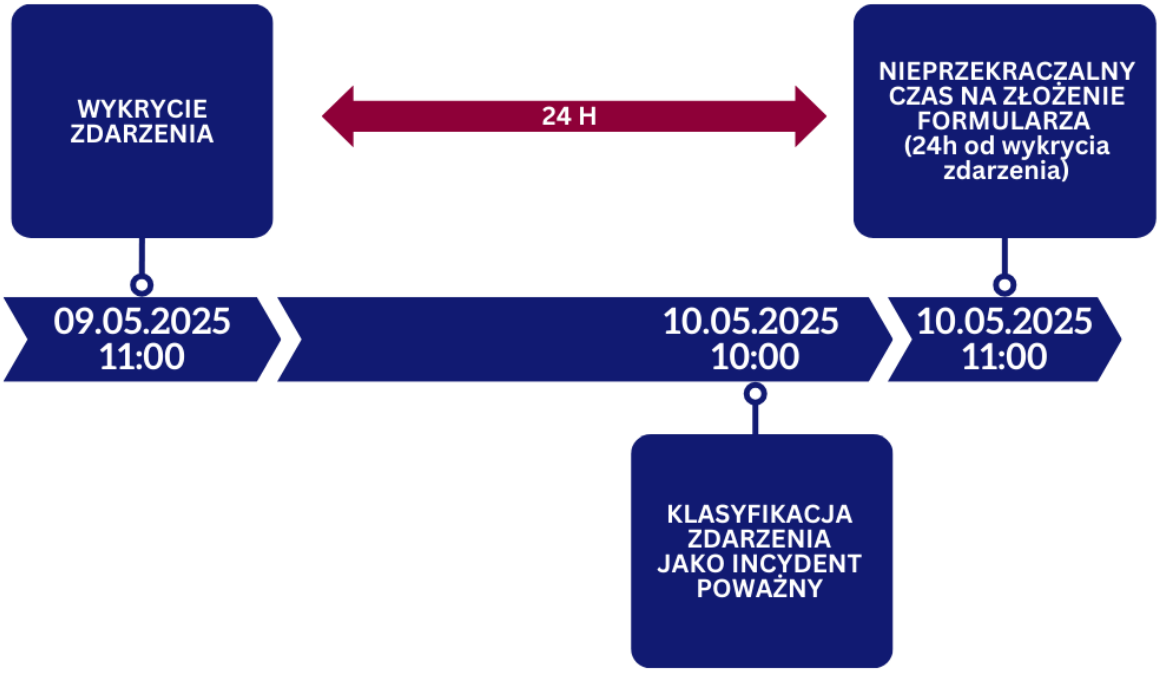
PRZYKŁADY:

- dla podpunktu „a” – 4h na wypełnienie formularza od klasyfikacji zdarzenia jako incydent poważny (rys. 1):



Rysunek 1 Czas na zgłoszenie incydentu 1/2

- dla podpunktu „b” – max 24h na wypełnienie formularza od wykrycia zdarzenia (rys. 2):



Rysunek 2 Czas na zgłoszenie incydentu 2/2

2. Sprawozdanie śródokresowe składane jest **do 72 godzin** od zgłoszenia wstępnego powiadomienia.
3. Sprawozdanie końcowe składane jest **do 30 dni** od daty złożenia ostatniego sprawozdania śródokresowego.

Formularz podzielony jest na wymienione wyżej 3 etapy. Należy zwrócić uwagę na to, że zawiera on pola wymagane do uzupełnienia, bez których nie ma możliwości złożenia formularza. Przy czym pola obligatoryjne zależą od rodzaju zgłaszanego incydentu i zawartych informacji. W razie nieuzupełnienia wymaganego pola, walidator zaszyty w formularzu poinformuje o tym przy próbie zapisania zgłoszenia. Istnieje również możliwość uzupełnienia pól z innego etapu, które w tym momencie nie są traktowane jako obligatoryjne np. elementy wymagane w trakcie składania sprawozdania śródokresowego, nie są niezbędne, ale możliwe do uzupełnienia w trakcie wypełnienia wstępnego powiadomienia. Ważne jest jednak, aby w trakcie dokonywania zgłoszenia przekazać jak najszerszy obraz zdarzenia, ponieważ wpływa to na możliwość podejmowanych działań przez regulatora.

Dodatkowo pierwsze sprawozdanie śródokresowe powinno być złożone z zachowaniem ustawowych terminów. Rozporządzenie DORA zakłada możliwość okresowej aktualizacji statusu incydentu, poprzez składanie aktualizacji sprawozdania śródokresowego.

W trakcie obsługi incydentu zgłaszający może dokonać reklasyfikacji, także jeżeli analiza wykaże, że incydent nie spełnia jednak wymagań incydentu poważnego.

W przypadku braku możliwości złożenia zgłoszenia przy wykorzystaniu Systemu Obsługi Incydentów DORA (SOID), podmiot nie jest zwolniony z obowiązku zaraportowania incydentu w ramach obligatoryjnych norm czasowych. W takim przypadku na stronie internetowej UKNF należy odszukać formularz obsługi incydentów DORA (plik w formacie xlsx) i po wypełnieniu go, przekazać do CSIRT KNF, poprzez przesłanie mailowej informacji na adres incydenty.dora@knf.gov.pl. Klucz PGP do zabezpieczenia wiadomości znajduje się pod adresem: https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Klucz_PGP. Po odzyskaniu dostępu do systemu SOID należy wypełnić zgłoszenia w systemie, uwzględniając informację o przekazaniu formularza drogą mailową.

2. Zakładanie konta i logowanie do Systemu Obsługi Incydentów DORA

*Przed przystąpieniem do rejestracji należy upewnić się, że użytkownik posiada aktywny **Profil Zaufany**. Można to zweryfikować, logując się na stronę Profilu Zaufanego (https://pz.gov.pl/pz/index) lub do systemu publicznego, który umożliwia korzystanie z tej formy uwierzytelniania. W przypadku braku Profilu Zaufanego, należy go założyć.*

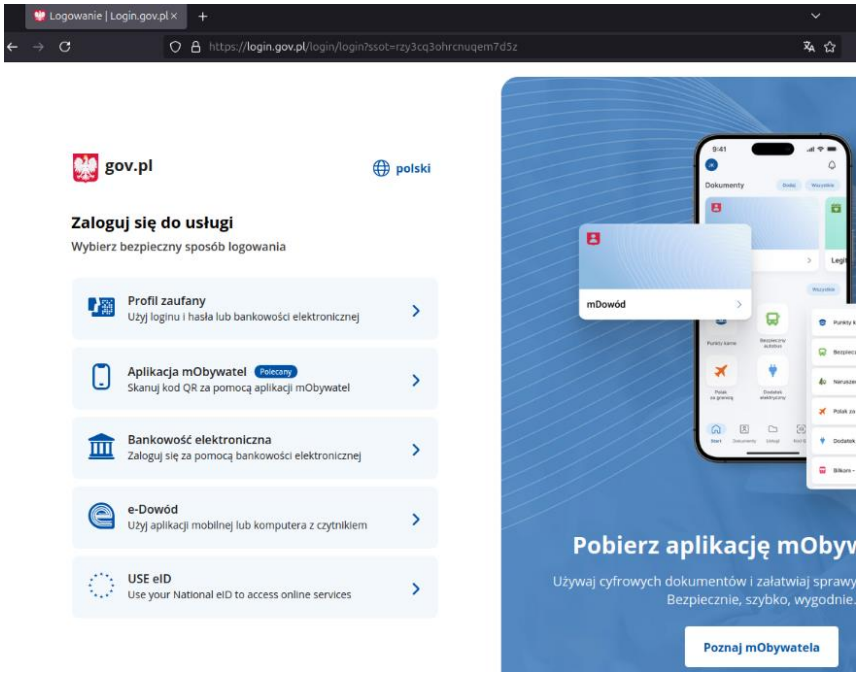
System zgłaszania incydentów znajduje się pod adresem https://csirt.knf.gov.pl.

Po wejściu na stronę użytkownik zostaje przekierowany na stronę główną. W celu rozpoczęcia procesu rejestracji w systemie zgłaszania incydentów poważnych należy kliknąć przycisk **„Rejestracja”.**

Po kliknięciu **„Rejestracja”** należy wybrać **„Zaloguj”.** Użytkownik zostanie przekierowany do procesu uwierzytelnienia w systemie za pomocą Profilu Zaufanego (rys. 3).

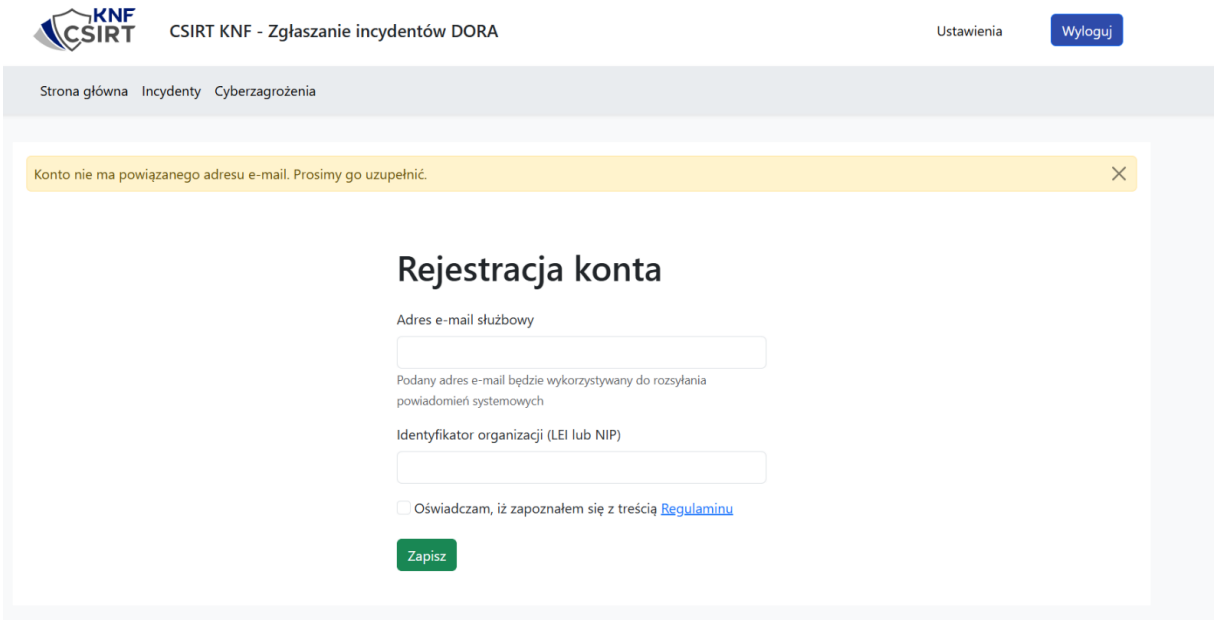
Rysunek 3 Rejestracja użytkownika do portalu

Użytkownik zostanie przekierowany na stronę **login.gov.pl**, która jest oficjalnym serwisem umożliwiającym logowanie za pomocą Profilu Zaufanego (rys.4).



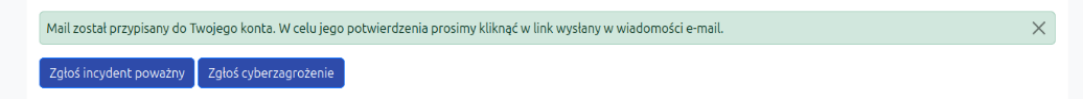
Rysunek 4 Rejestracja z wykorzystaniem Profilu Zaufanego

Po pomyślnym zalogowaniu za pomocą Profilu Zaufanego użytkownik zostanie automatycznie przekierowany z powrotem na stronę https://csirt.knf.gov.pl. Następnie system wyświetli formularz, w którym użytkownik zostanie poproszony o podanie służbowego adresu e-mail oraz kodu LEI (rys. 5).



Rysunek 5 Ostatni etap rejestracji użytkownika

Po wprowadzeniu służbowego adresu e-mail użytkownik otrzyma komunikat potwierdzający, informujący o poprawnym zapisaniu danych. Dodatkowo należy potwierdzić adres e-mail poprzez kliknięcie w link aktywacyjny, który zostanie wysłany na podany adres e-mail (rys. 6).



Rysunek 6 Potwierdzenie rejestracji użytkownika

Po pomyślnym potwierdzeniu adresu e-mail użytkownik uzyskuje możliwość zalogowania się do systemu. Aby to zrobić, należy przejść na stronę główną systemu i kliknąć przycisk **„Zaloguj”** (rys. 7).

Rysunek 7 Logowanie do portalu

Po zalogowaniu za pomocą Profilu Zaufanego użytkownik zostanie automatycznie przekierowany do panelu zarządzania incydentami.

3. Role w panelu zarządzania incydentami

W tym panelu dostępne są dwie role: użytkownika oraz koordynatora. W zależności jakie uprawnienia posiadamy, będziemy mieli możliwość podejmowania poszczególnych czynności.

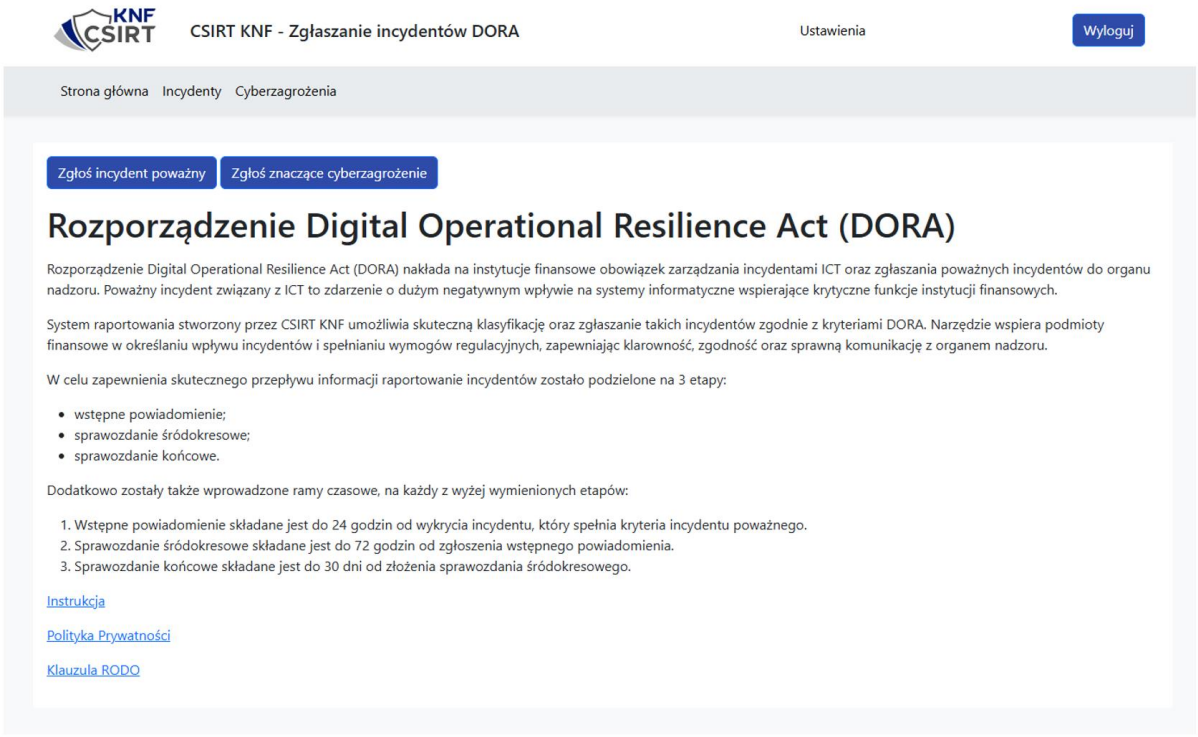
Funkcja użytkownika umożliwia zgłaszanie, przeglądanie oraz zarządzanie incydentami w systemie, tymi których autorem jest ten sam użytkownik. Natomiast rola koordynatora zawiera funkcje użytkownika oraz dodatkowo:

- możliwość dodawania osób przypisanych do organizacji, a także ich usuwania,
- podglądu zgłoszeń osób dodanych do organizacji, którą koordynuje.

Bez różnicy na przyjmowaną rolę, w panelu „Ustawienia” (prawy, górny róg) można zaznaczyć opcję „Powiadomienia e-mail”, co będzie skutkować informacjami mailowymi o zbliżających się i przekroczonych terminach zgłoszeń incydentów.

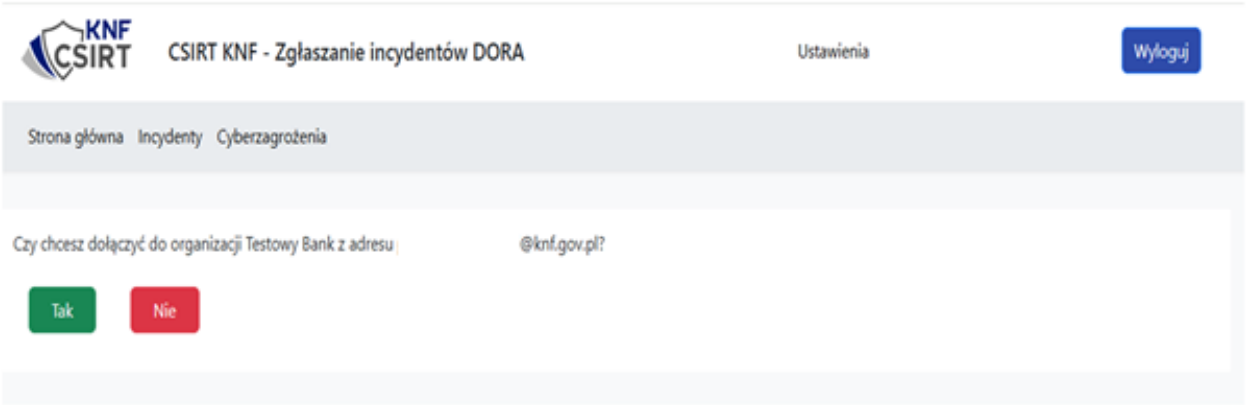
3.1 Dostęp w roli użytkownika

Widok panelu z dostępem użytkownika (rys. 8).



Rysunek 8 Widok portalu z roli użytkownika

Użytkownik dołącza do organizacji poprzez wiadomość e-mail z systemu, zainicjonowaną działaniem koordynatora. Po kliknięciu w link w wiadomości i zalogowaniu się do portalu, użytkownik zostanie zapytany o chęć dołączenia do konkretnej organizacji (rys. 9), w przypadku wyrażenia takiej zgody, zostanie do niej przyłączony.



Rysunek 9 Etap dołączania użytkownika do organizacji

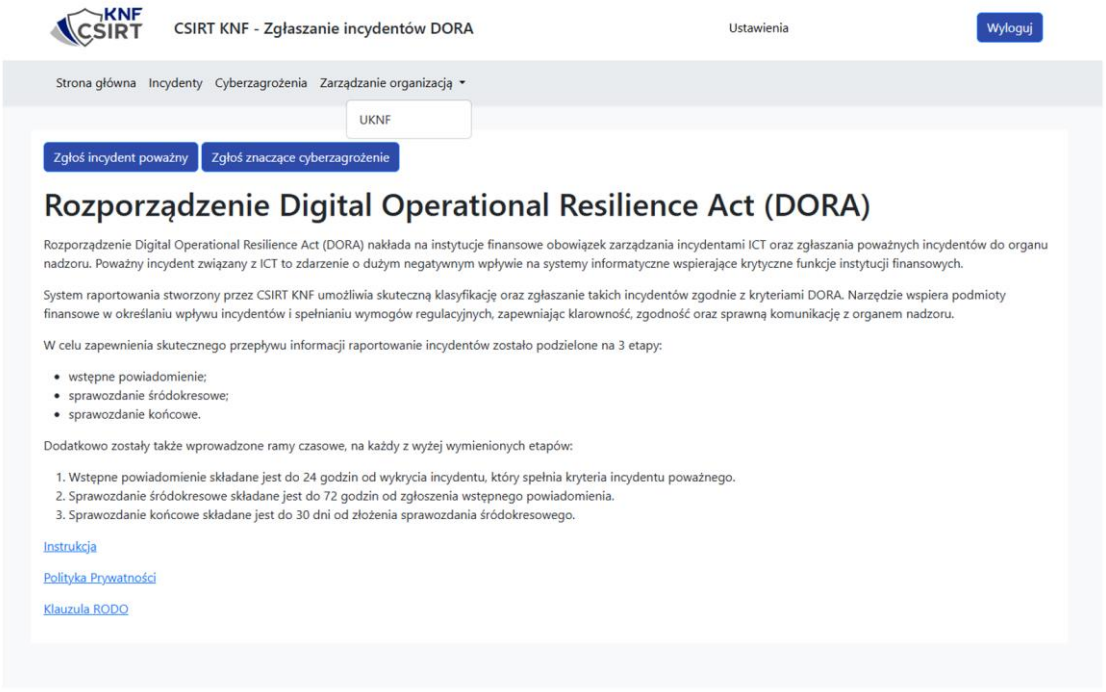
W trakcie pracy w systemie użytkownik będzie miał dostęp do wszystkich zrobionych przez siebie zgłoszeń, a w trakcie obsługi incydentu, będzie miał również możliwość edytowania zawartych informacji.
Ważne jest, aby użytkownik pamiętał o usunięciu siebie samego z listy danej organizacji, w przypadku np. zmiany organizacji którą reprezentowaliśmy. To ważne, ponieważ w roli użytkownika, raportowanie może odbywać się tylko w ramach jednej organizacji. W przypadku np. zmiany pracodawcy, brak usunięcia się z listy poprzedniej firmy uniemożliwi dokonywanie zgłoszeń dla nowego podmiotu.

3.2 Dostęp w roli koordynatora

Rola koordynatora nie jest obligatoryjna do założenia dla konkretnej organizacji. Istotnie pomaga jednak zarządzić procesem reagowania na incydenty bezpieczeństwa w przypadku jeżeli zgłoszeniami zajmuje się lub może zajmować (zastępowalność) więcej niż jedna osoba. Rola koordynatora nie jest potrzebna, w sytuacji gdy w organizacji tylko jedna osoba będzie składać informacje dotyczące wystąpienia incydentu np. w przypadku jednoosobowych działalności gospodarczych.

Innym przypadkiem, kiedy może zostać nadana rola koordynatora w systemie, to sytuacja gdy użytkownik jest przedstawicielem kilku podmiotów i w ich imieniu może składać raporty. W tej sytuacji, rola koordynatora pozwoli mu, na zarządzanie, w ramach której organizacji w danym momencie przekazywane są informacje.

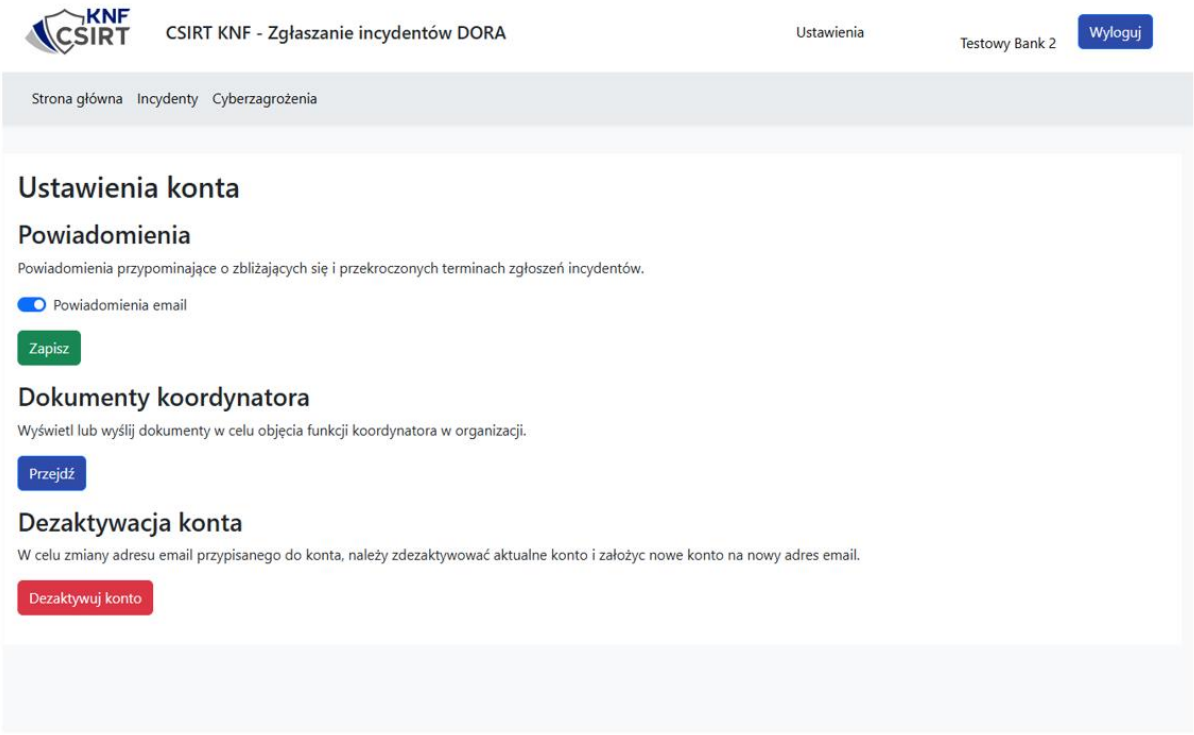
Widok panelu z dostępem koordynatora, od dostępu użytkownika różni się zakładką „Zarządzanie organizacją” (rys. 10).



Rysunek 10 Widok portalu w roli koordynatora

3.2.1 Uzyskanie i odwołanie funkcji koordynatora

Aby utworzyć rolę koordynatora w organizacji należy złożyć wniosek poprzez formularz zgłaszania incydentu (https://csirt.knf.gov.pl/). Po przejściu procesu logowania, należy przejść do „Ustawienia" w prawym górnym rogu panelu i wybrać opcję „Dokumenty koordynatora" (rys. 11).



Rysunek 11 Pozyskiwanie roli koordynatora

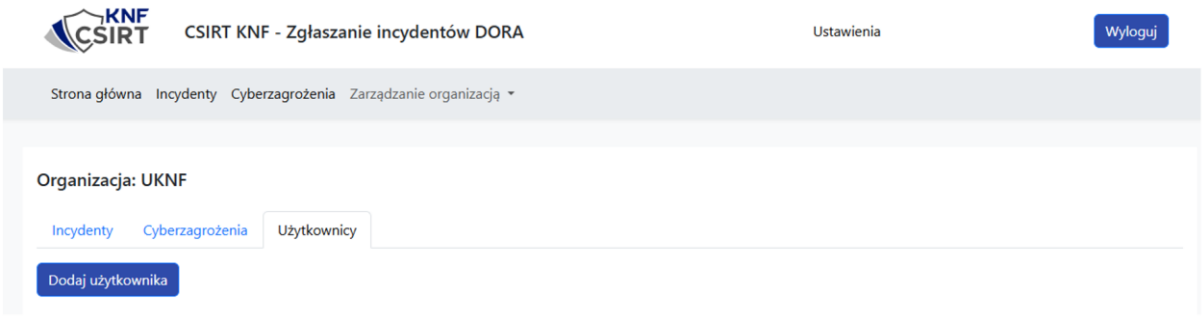
W następnym kroku następuje wgranie, w formie pliku, wniosku objęcia funkcji koordynatora. Wzór dokumentu dostępny jest w systemie SOID. **Wgrywany plik musi mieć format PDF.** Po dodaniu dokumentu na adres użytkownika przesyłane jest mailowe potwierdzenie przyjęcia dokumentu. Należy mieć na uwadze, że weryfikacja przekazanych dokumentów odbywa się manualnie, co wpływa na czas rozpatrywania wniosku.

Wycofanie funkcji koordynatora następuje poprzez zgłoszenie tej informacji, w postaci wiadomości e-mail skierowanej na adres: incydenty.dora@knf.gov.pl

3.2.2 Dodanie użytkownika do organizacji

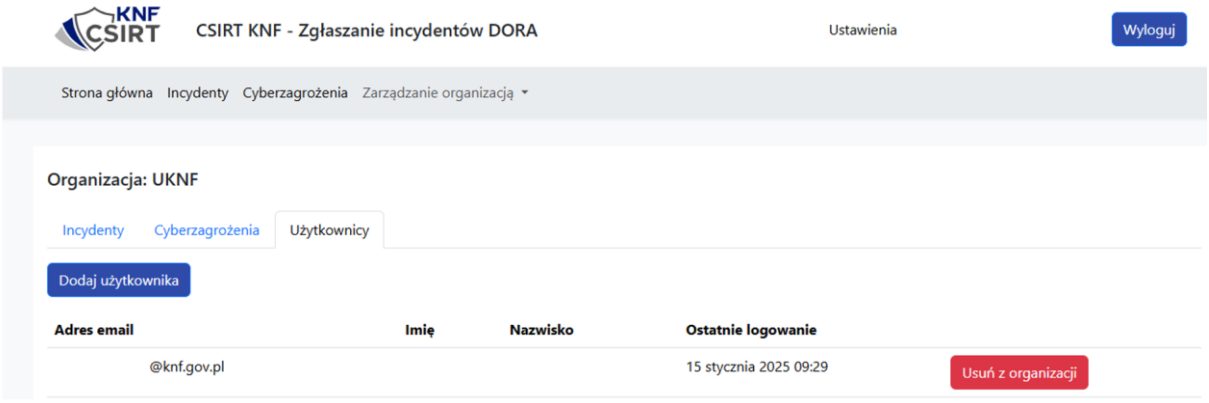
Jedną z funkcji koordynatora jest możliwość dodawania użytkowników do organizacji. Zanim to nastąpi, użytkownik musi zadbać wcześniej o utworzenie konta dla siebie. Proces dodawania użytkownika

odbywa się w zakładce „Zarządzanie organizacją”, w sekcji „Użytkownicy”. Następnie wybieramy „Dodaj użytkownika”(rys. 12).



Rysunek 12 Dodawanie użytkownika przez koordynatora

Użytkownik otrzyma wiadomość e-mail z zaproszeniem dołączenia do organizacji. Po jego zaakceptowaniu koordynator otrzyma powiadomienie e-mail o zaakceptowaniu przez użytkownika zaproszenia. Od tego momentu w panelu koordynatora widoczny będzie dodany użytkownik (rys. 13).



Rysunek 13 Lista użytkowników

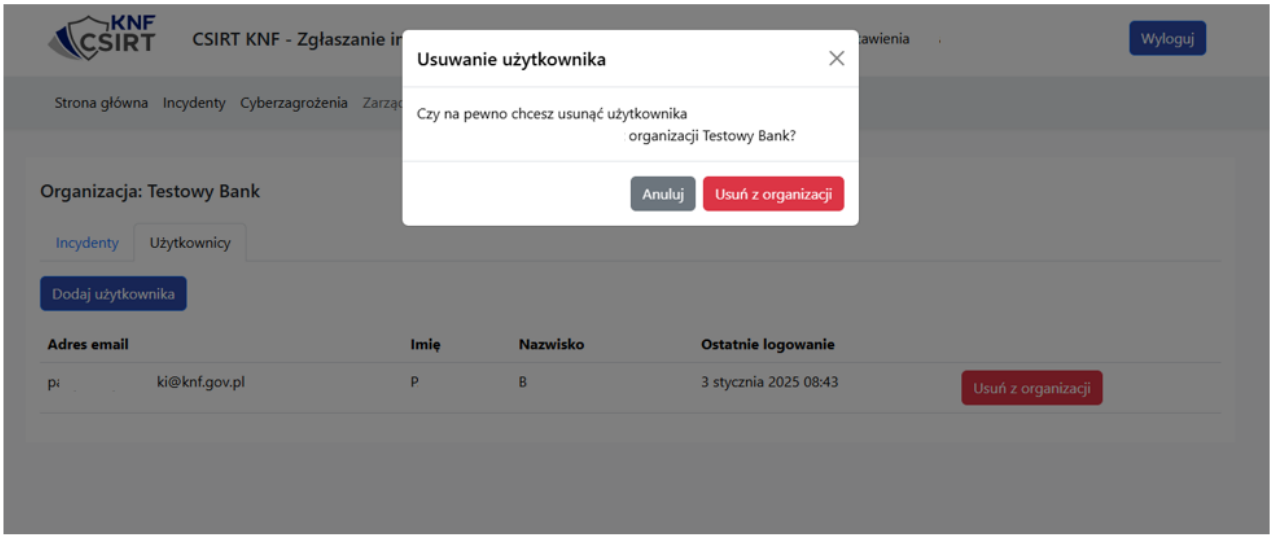
Należy mieć na uwadze, że wgląd w składane formularze w imieniu danej organizacji, będziemy mieli dopiero w momencie, kiedy dany użytkownik zostanie dodany do listy naszej organizacji. Ważnym jest zatem, żeby jako koordynator organizacji, utrzymywać zaktualizowaną listę osób, które składają informacje o incydentach poważnych w systemie. Pozwoli to zachować porządek w zarządzaniu zdarzeniami.

3.2.3 Usuwanie użytkownika z organizacji

Koordynator może usuwać użytkowników z organizacji za pomocą przycisku „Usuń z organizacji”, dostępnego w zakładce „Zarządzanie organizacją”, w sekcji „Użytkownicy”.

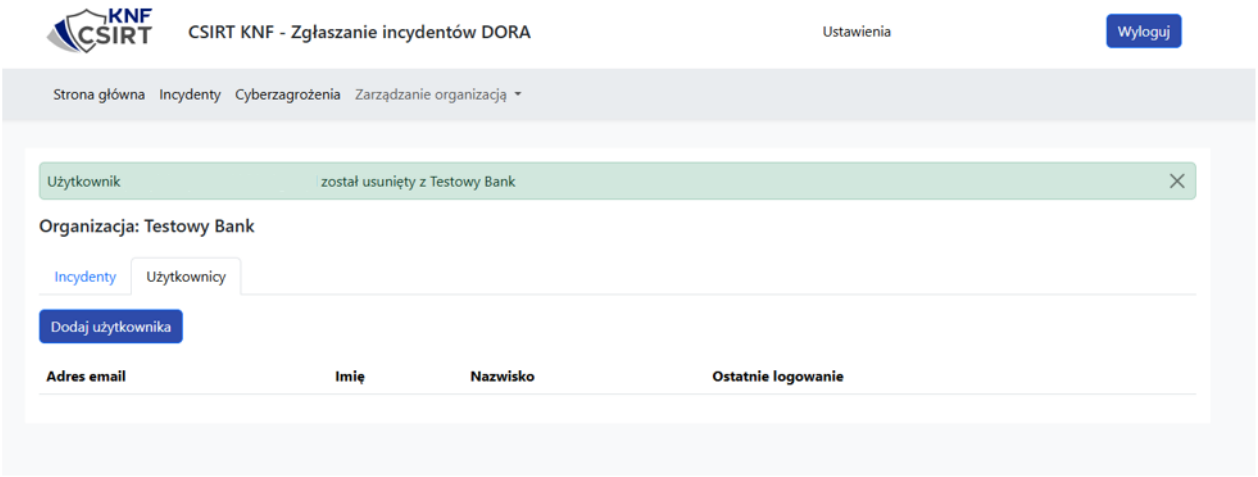
WAŻNE: Usunięcie użytkownika z organizacji dezaktywuje jego konto w systemie.

Po wybraniu przycisku „Usuń z organizacji”, system poprosi o potwierdzenie podjętego działania (rys. 14).



Rysunek 14 Usuwanie użytkownika z listy 2/2

Następnie użytkownik zostanie usunięty z listy, a jego konto nie będzie już aktywne (rys. 15).



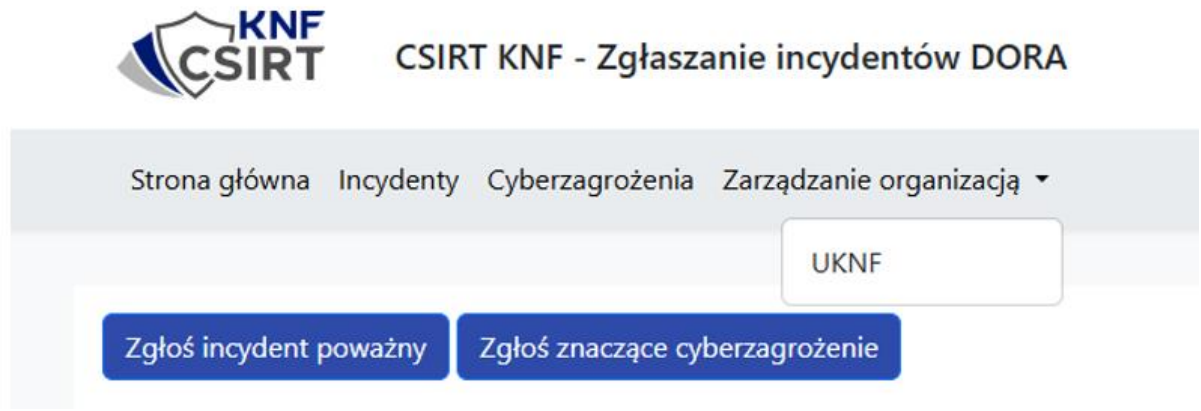
Rysunek 15 Potwierdzenie usunięcia użytkownika

4. Zgłoszenie incydentu poważnego przy pomocy formularza

4.1 Pierwsze kroki w zgłoszeniu incydentu

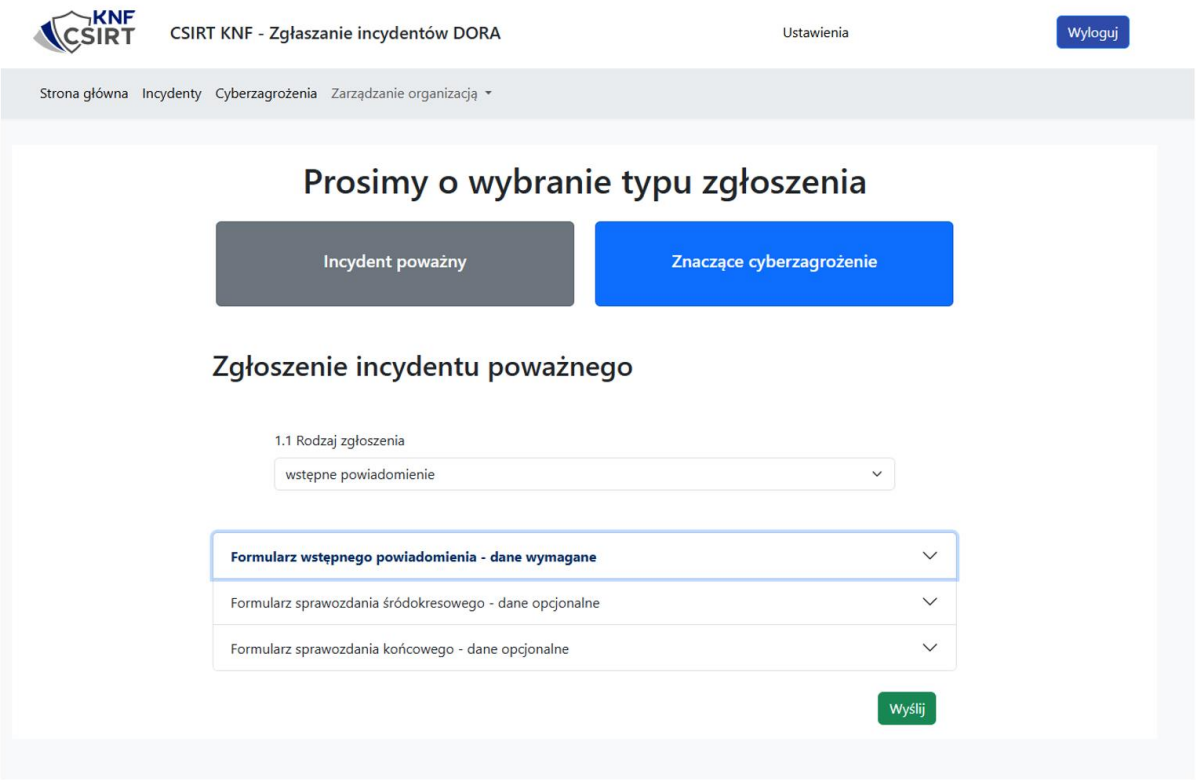
Po zalogowaniu do panelu, w zależności od tego jaka została przypisana nam rola (patrz wyżej), muszą zostać podjęte odpowiednie kroki.

W przypadku roli koordynatora, należy wejść w opcję „Zarządzanie organizacją" i wybrać tę, w imieniu której złożony zostanie formularz informujący o incydencie (rys. 16). Następnie należy wybrać rodzaj zdarzenia, który chcemy zgłosić.



Rysunek 16 Zgłoszenie incydentu - widok z roli koordynatora

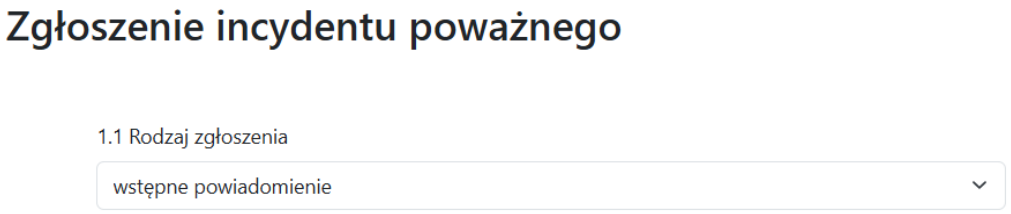
W przypadku roli użytkownika, pominięty zostanie pierwszy krok, przechodząc od razu do wyboru rodzaju zdarzenia, którego dotyczy zgłoszenie. W przypadku tej instrukcji, każdorazowo będzie to „Zgłoś incydent poważny". Następnie zgłaszający zostanie przekierowany do przedmiotowego formularza (rys. 17).



Rysunek 17 Zgłoszenie incydentu - widok z roli użytkownika i koordynatora

Pole „wyszarzone" wskazuje na rodzaj zgłoszenia, które dokonujemy, w przypadku powyższego screenshota formularz dotyczy „Incydentu poważnego".

W tym kroku wybrać należy rodzaj zgłoszenia, którego dokonujemy (wstępne powiadomienie, sprawozdanie śródokresowe, sprawozdanie końcowe). Rodzaje poszczególnych zgłoszeń opisane zostały w pierwszym rozdziale tego dokumentu (rys. 18).



Rysunek 18 Wybór rodzaju zgłoszenia

Po wybraniu rodzaju zgłoszenia, formularz zaznaczy, które formularze są wymagane do uzupełnienia. To oznacza, że w przypadku wybrania „Wstępne powiadomienie" system zaznaczy nam „Formularz wstępnego powiadomienia" jako wymagany do uzupełnienia (rys. 19).

Rysunek 19 Podkreślenie formularzy obowiązkowych do wypełnienia ½

Natomiast w przypadku wyboru „Sprawozdanie śródokresowe" system jako wymagane do uzupełnienia wskaże „Formularz wstępnego powiadomienia" oraz „Formularz sprawozdania śródokresowego" (rys. 20).

Rysunek 20 Podkreślenie formularzy obowiązkowych do wypełnienia 2/2

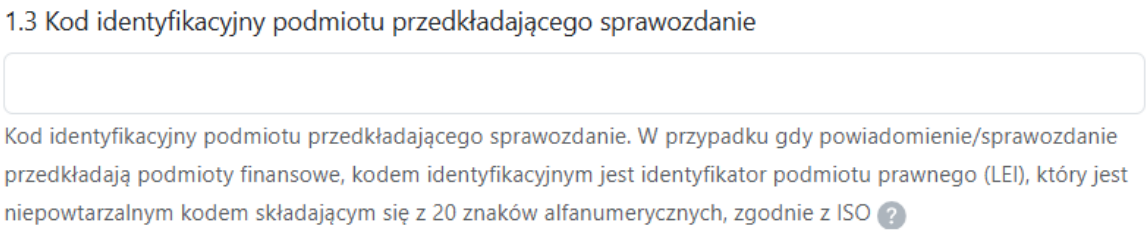
Analogiczna sytuacja będzie miała miejsce w przypadku wybrania sprawozdania końcowego.

4.2 Formularz wstępnego powiadomienia

W tej sekcji formularz zawiera informacje ogólne o organizacji. Ważnym jest prawidłowe wypełnienie danych jakiego podmiotu dotyczy incydent.

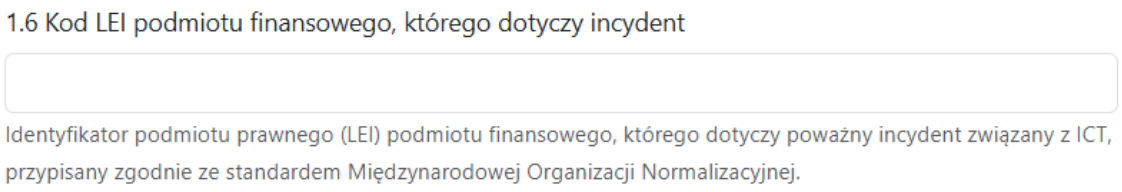
Uwaga dla osób składających sprawozdanie w imieniu organizacji trzeciej

Pole 1.3 (rys. 21):



Rysunek 21 Identyfikacja zgłaszającego incydent

I 1.6 (rys. 22):



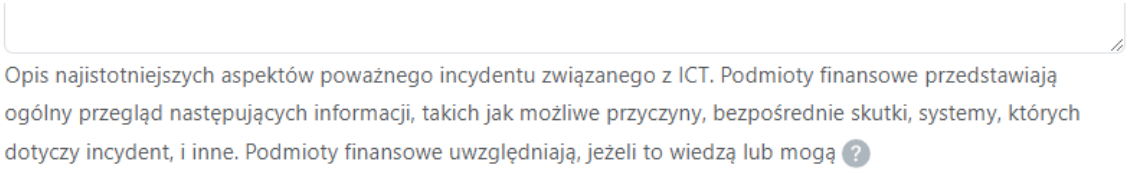
Rysunek 22 Kod LEI podmiotu, w którym wystąpił incydent

Zostaną uzupełnione tą samą daną (numerem LEI), tylko w wypadku jeżeli zgłaszający jest pracownikiem organizacji, w której wystąpił incydent. W innym wypadku w polu 1.3 należy wskazać dane identyfikujące zgłaszającego i nie musi być to numer LEI (jeżeli zgłaszający nie posiada). W tym miejscu można uzupełnić pole wpisując NIP, REGON lub inną daną umożliwiająca identyfikację podmiotu. W polu 1.6 kod LEI podmiotu finansowego, którego dotyczy incydent jest wymagany.

W przypadku sprawozdawczości zagregowanej, czyli zgłaszania wystąpienia tego samego incydentu w więcej niż jednym podmiocie w polu 1.4 należy wybrać wszystkie rodzaje podmiotów finansowych objętych sprawozdawczością zagregowaną (pole wielokrotnego wyboru). Natomiast w polu 1.5 i 1.6 składający sprawozdanie wpisuje wszystkie nazw podmiotów finansowych, których dotyczy poważny incydent związany z ICT, oddzielając wpisy średnikiem. Kolejność podawania kodów LEI i nazw podmiotów finansowych musi być identyczna.

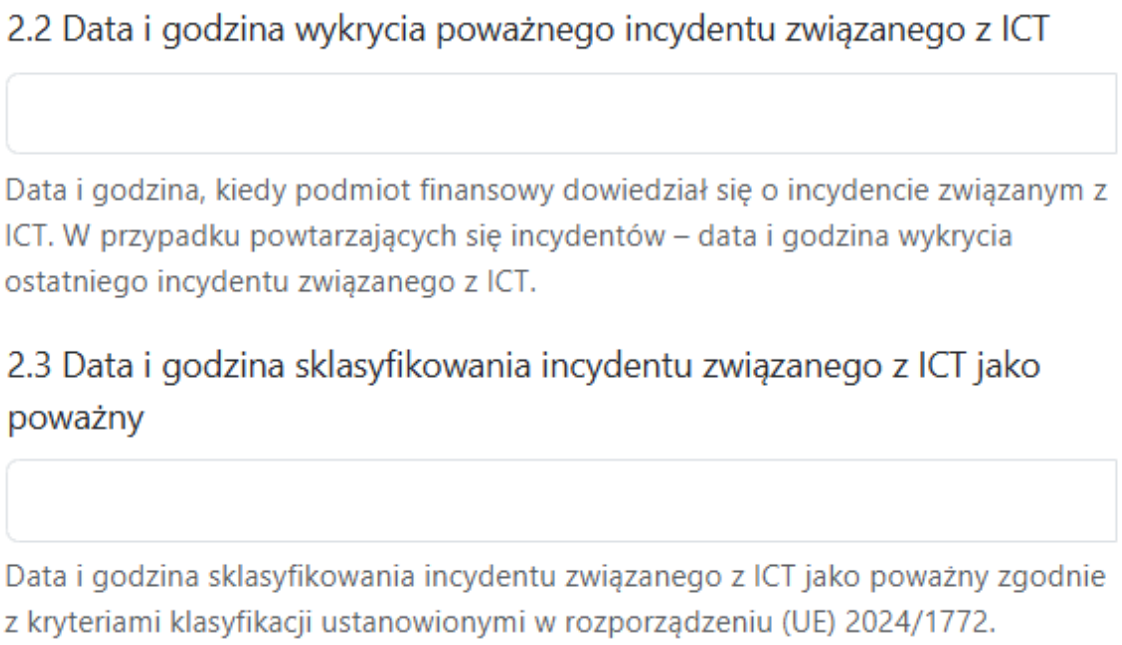
Uwaga dla wszystkich osób składających sprawozdanie w imieniu organizacji trzeciej

Formularz wstępnego powiadomienia zawiera również podstawowe informacje o zdarzeniu, dające podgląd na raportowany incydent. Należy zwrócić uwagę na opisy znajdujące się pod poszczególnymi polami do uzupełnienia. Zaczerpnięte zostały z Regulatory Technical Standards (RTS) EBA. Dodatkowo, każdorazowo gdy opis ten zawiera „ikonkę znaku zapytania", to po jej kliknięciu pojawi się szczegółowy opis pola (rys. 23).



Rysunek 23 Rozwinięcie opisu pola formularza

W sekcji „Dane opisujące i klasyfikujące incydent" znajdują się pola 2.2 Data i godzina wykrycia poważnego incydentu związanego z ICT oraz 2.3 Data i godzina sklasyfikowania incydentu związanego z ICT jako poważny (rys. 24).



Rysunek 24 Klasyfikacja czasu zgłaszania incydentu poważnego

Należy pamiętać, że w przypadku wykrycia zdarzenia, podmiot finansowy ma 24h na zakwalifikowanie zdarzenia jako incydent poważny i uzupełnienie formularza (co najmniej „Formularz wstępnego powiadomienia"). Natomiast po zakwalifikowaniu zdarzenia jako incydent poważny, podmiot finansowy ma 4h na uzupełnienie wspomnianego wyżej formularza. Mając jednocześnie na uwadze, że samo wypełnienie formularza nie może odbyć się później niż 24h od wykrycia zdarzenia.

Po wypełnieniu powyższego formularza i kliknięciu przycisku „Wyślij”, należy zwrócić uwagę, czy system nie poinformował o niewypełnieniu pól obligatoryjnych (rys. 25).

Rysunek 25 Działanie walidatora

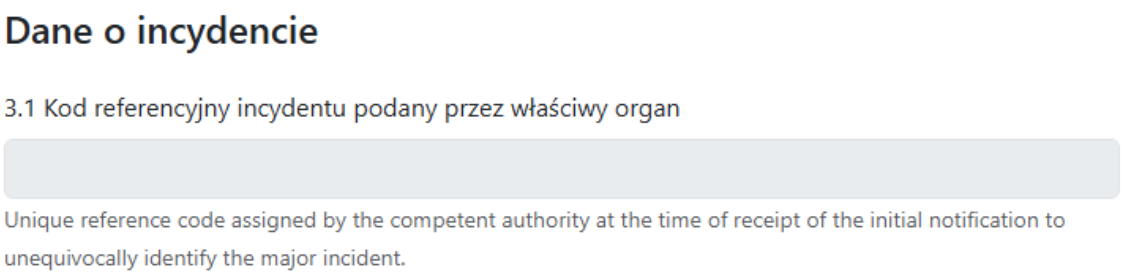
W przypadku braku ich uzupełnienia formularz nie zostanie przekazany do regulatora, co jest równoznaczne z brakiem zaraportowania informacji o incydencie.

4.3 Formularz sprawozdania śródokresowego

Sprawozdanie śródokresowe jest uzupełnieniem wstępnego powiadomienia. Oznacza to, że raport ten należy poprzez kliknięcie w górnym panelu przycisku „Incydenty”. A następnie wybranie z listy zdarzenia, które chcemy uzupełnić.

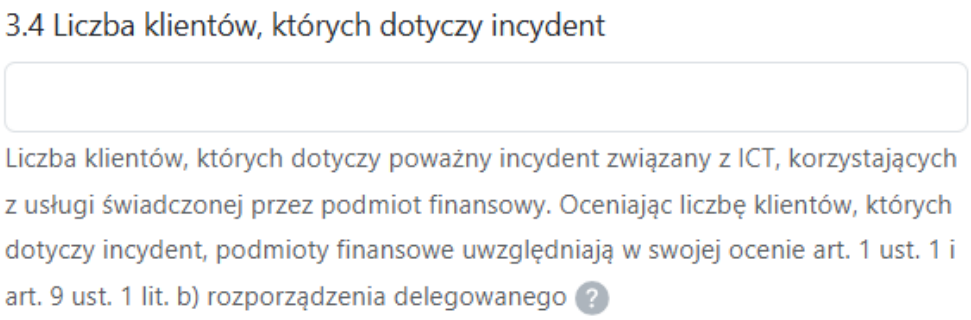
Sprawozdanie śródokresowe należy złożyć do 72 godzin po złożeniu wstępnego powiadomienia.

W pierwszym polu tego formularza zawarty zostanie Kod referencyjny incydentu podany przez regulatora, w celu jednoznacznej identyfikacji poważnego incydentu związanego z ICT. Osoba składająca sprawozdanie o incydencie nie uzupenia tego pola. Kod ten zostaje nadany po przekazaniu do regulatora „Wstępnego powiadomienia”. Jeżeli zgłaszający od razu uzupełnia więcej niż Formularz wstępnego powiadomienia (czyli dodatkowo Formularz sprawozdania śródokresowego i/lub Formularz sprawozdania końcowego) pole to pozostanie puste (rys. 26).



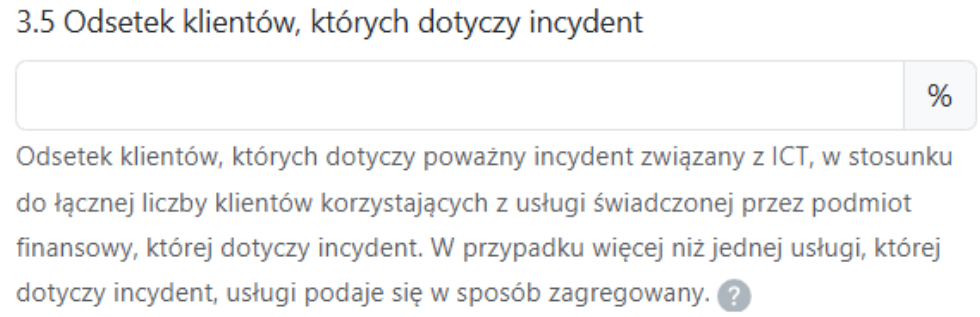
Rysunek 26 Pochodzenie kodu referencyjnego incydentu

Dla pola 3.4 Liczba klientów, których dotyczy incydent w przypadku sprawozdawczości zagregowanej, należy wpisać łączną liczbę klientów, których dotyczy incydent, we wszystkich podmiotach finansowych (rys. 27).



Rysunek 27 Klasyfikacja liczenia klientów dotkniętych incydentem

Dla pola 3.5 Odsetek klientów, których dotyczy incydent w przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, podmiot finansowy dzieli sumę wszystkich klientów, których dotyczy incydent, przez łączną liczbę klientów wszystkich podmiotów finansowych, których dotyczy incydent (rys. 28).

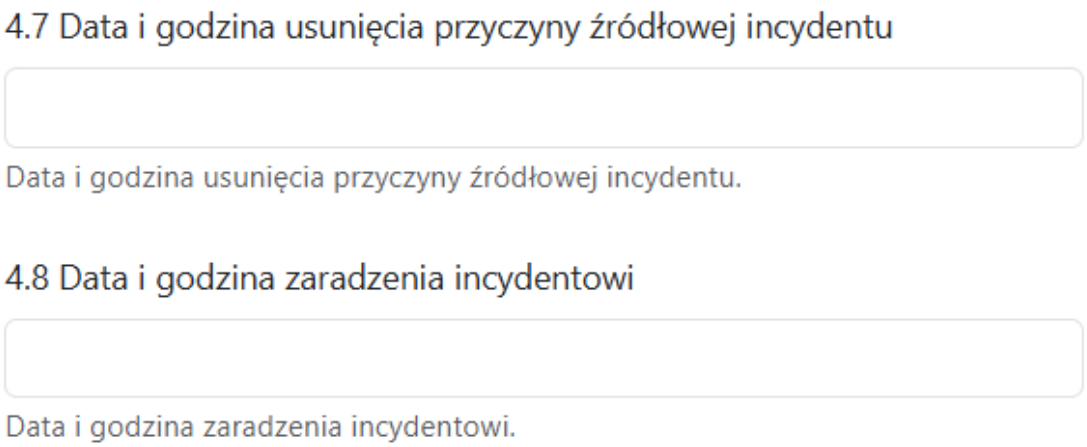


Rysunek 28 Wyliczenie odsetku klientów dotkniętych incydentem

W kolejnych punktach analogicznie w przypadku sprawozdawczości zagregowanej należy uwzględniać liczby będące sumą konkretnej danej we wszystkich podmiotach finansowych objętych zgłoszeniem.

4.4 Formularz sprawozdania końcowego

Ta sekcja zawiera pola 4.7 Data i godzina usunięcia przyczyny źródłowej incydentu oraz 4.8 Data i godzina zaradzenia incydentowi (rys. 29).



Rysunek 29 Czas usunięcia, a powrotu do stanu sprzed incydentu

W tym wypadku w polu 4.7 należy wpisać czas, kiedy przyczyna wystąpienia incydentu została usunięta, natomiast w polu 4.8 moment, w którym organizacja wróciła do stanu działania sprzed wystąpienia incydentu.

Po wypełnieniu wszystkich wymaganych pól i przekazaniu formularza zgłaszający otrzyma komunikat o zgodności walidatora w uzupełnianych polach w formularzu, a także przekazana zostanie automatyczna wiadomość e-mail potwierdzająca złożenie zgłoszenia.

Tabela zmian:

Lp.	Treść zmiany	Data zmiany
1	Wersja ustalona do publikacji	08/01/2025
2	XXXXXXX	

Spis ilustracji

Znaczenie kolorów TLP dla odbiorców wiadomości

TLP: RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem odbiorców tych wiadomości.
TLP: AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie **TLP:AMBER+STRICT** , które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.
TLP: GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.
TLP: CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).