1. IS.I.OR.245 Prowadzenie rejestrów

Urząd Lotnictwa Cywilnego

02.09.2025

IS.I.OR.245 (IS.AR.230) - PROWADZENIE REJESTRÓW

1. Organizacja prowadzi rejestr swoich działań w zakresie zarządzania bezpieczeństwem informacji

W tym celu powinna ustanowić **Politykę przechowywania danych**, **która** wyjaśnia, jakie informacje powinny być przechowywane lub archiwizowane oraz przez jaki okres.

Polityka przechowywania danych określa procedury mające na celu:

- zarządzanie odpowiednimi plikami danych dotyczących bezpieczeństwa;
- ustanowienie okresowej oceny ich zawartości;
- określenie kryteriów umożliwiających usuwanie zapisów zdarzeń związanych z bezpieczeństwem informacji, gdy cel ponownej oceny tych zdarzeń został osiągnięty.

Ilość informacji, które należy dokumentować w celu zachowania zgodności z celami Rozporządzenia KE (UE) 2023/203 może się różnić w zależności od organizacji, ze względu jej wielkość i złożoność lub potrzebę harmonizacji z innymi już istniejącymi procesami zarządzania

IS.I.OR.245 (IS.AR.230) - PROWADZENIE REJESTRÓW

a) Archiwizacja możliwych do zidentyfikowania zapisów obejmuje:

- otrzymane zatwierdzenia wraz z powiązanymi ocenami ryzyka,
- umowy zlecenia innym organizacjom jakichkolwiek czynności związanych z ISMS/SZBI,
- rejestry najważniejszych procesów/procedur/funkcji i obowiązków,
- dokumentację ryzyka zidentyfikowanego w ocenie ryzyka wraz z zidentyfikowanymi środkami zmniejszenia ryzyka,
- dokumentację incydentów związanych z bezpieczeństwem informacji i podatności zgłoszonych za pośrednictwem wewnętrznych systemów zgłaszania zdarzeń,
- dokumentację zdarzeń związanych z bezpieczeństwem informacji, które mogą wymagać ponownej oceny w celu identyfikacji niewykrytych incydentów związanych z bezpieczeństwem informacji lub podatności.

IS.I.OR.245 (IS.AR.230) - PROWADZENIE REJESTRÓW

b) Okres przechowywania dokumentacji

- Co najmniej 5 lat:
  - od utraty ważności zatwierdzenia
  - od zmiany lub rozwiązania umowy dot. czynności zleconych
  - rejestry najważniejszych procesów/ dokumentacji ryzyka zidentyfikowanego w ocenie ryzyka / dokumentacji zgłoszonych incydentów związanych z bezpieczeństwem informacji

- Dokumentację zdarzeń wymagających ponownej oceny w celu identyfikacji niewykrytych incydentów przechowuje się do czasu ponownej oceny zdarzeń związanych z bezpieczeństwem informacji

IS.I.OR.245 (IS.AR.230) - PROWADZENIE REJESTRÓW

2. Organizacja prowadzi rejestry kwalifikacji i doświadczenia własnego personelu zaangażowanego w działania w zakresie zarządzania bezpieczeństwem informacji

   - Okres przechowywania ww. rejestrów – przez cały okres zatrudnienia członków personelu i min. 3 lata po opuszczeniu przez nich organizacji
   - Organizacja zapewnia dostęp do akt osobowych dla członków personelu, a w chwili opuszczania przez nich organizacji, na żądanie przekazuje egzemplarz akt osobowych

3. Organizacja określa format dokumentacji

4. Organizacja zapewnia ochronę rejestrów przed ich uszkodzeniem, zmianą i kradzieżą oraz określa klasyfikację poziomu klauzuli tajności (jeśli dotyczy). Przechowywanie rejestrów jest zapewnione w sposób gwarantujący ich integralność, autentyczność i uprawniony dostęp

IS.I.OR.245 (IS.AR.230) - PROWADZENIE REJESTRÓW

Praktyczne wskazówki dotyczące ochrony prowadzonych rejestrów danych:

- Stosowanie najlepszych praktyk przechowania danych (m. in. tworzenie kopii zapasowych w różnych lokalizacjach, w trybie offline, itp.). Praktyki te warto również stosować powierzając prowadzenie dokumentacji usługodawcom dysponującym rozproszonymi zasobami
- Przechowywanie danych, aby były dostępne i czytelne (np. określony system plików, format plików aplikacji, kompatybilne wersje baz danych, itp.)
- Ochrona danych w formie papierowej (np. ochrona przed nadmiernym ciepłem, światłem, wilgocią)
- Zapewnienie autentyczności i integralności poprzez stosowanie podpisów cyfrowych na poziomie dokumentu
- Ochrona przed nieuprawnionym dostępem stosując np. zabezpieczenie pliku hasłem, ochronę dostępu do baz danych, udziałów plików, katalogów, itp.

2. IS.I.OR.250 Podręcznik zarządzania bezpieczeństwem informacji (ISMM)

Urząd Lotnictwa Cywilnego

02.09.2025

IS.I.OR.250 – PODRĘCZNIK ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (ISMM)

1. Organizacja opracowuje Podręcznik Zarządzania Bezpieczeństwem Informacji (ISMM)

➢ Zawartość podręcznika:

- oświadczenie kierownika odpowiedzialnego
- tytuły, nazwiska, imiona, zakresy odpowiedzialności, zadania i uprawnienia osób kluczowych (odpowiedzialnych za zapewnienie zgodności z wymaganiami oraz zarządzanie funkcją monitorowania zgodności) oraz pozostałego personelu odpowiedzialnego za realizację ISMS/SZBI
- stosowana strategia bezpieczeństwa informacji
- opis liczby i kategorii pracowników oraz systemu umożliwiającego planowanie dostępności pracowników
- schemat organizacyjny i powiązana struktura odpowiedzialności

IS.I.OR.250 – PODRĘCZNIK ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (ISMM)

- Zawartość podręcznika cd:
  - opis wewnętrznego systemu zgłaszania zdarzeń
  - procedury zapewnienia zgodności dot. dokumentacji, kontroli zlecanych czynności, zmian do podręcznika ISMM
  - szczegóły aktualnie zatwierdzonych alternatywnych sposobów spełnienia wymagań (jeśli dotyczy)

IS.I.OR.250 – PODRĘCZNIK ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (ISMM)

2. Organizacja przekazuje do zatwierdzenia przez właściwy organ pierwsze wydanie podręcznika zarządzania bezpieczeństwem informacji (ISMM)

3. Organizacja opracowuje procedurę zarządzania zmianami podręcznika zarządzania bezpieczeństwem informacji

Uwaga: Organizacja opracowuje - wymagającą zatwierdzenia przez właściwy organ - procedurę zarządzania zmianami w systemie zarządzania bezpieczeństwem informacji ISMS/SZBI (w tym zmianami podręcznika ISMM).
W przypadku zmian nieobjętych zakresem stosowania procedury Organizacja ubiega się o zatwierdzenie przez właściwy organ i po zatwierdzeniu wprowadza je zgodnie z określonymi warunkami.

02.09.2025

IS.I.OR.250 – PODRĘCZNIK ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (ISMM)

4. W ramach zintegrowanego systemu zarządzania ISMM może być włączony do innych charakterystyk lub podręczników zarządzania (np. Podręcznik zarządzania bezpieczeństwem, Podręcznik monitorowania zgodności) posiadanych przez Organizację, z zachowaniem wyraźnych odniesień wskazujących które części odnoszą się do poszczególnych wymagań dotyczących ISMS/SZBI

Uwaga: Jeżeli podmiot posiada wiele zezwoleń lub deklaracji, ISMM może mieć zastosowanie do jednej lub kilku organizacji jednocześnie w oparciu o wspólny ISMS.
ISMM powinien zawierać co najmniej dokument zatwierdzający każdej organizacji i powinien zostać formalnie zatwierdzony przez kierownika odpowiedzialnego lub osobę odpowiedzialną w każdej organizacji, chyba że dla wszystkich organizacji została delegowana wspólna osoba odpowiedzialna procesy i procedury w zakresie bezpieczeństwa informacji

5. Zalecane jest ustanowienie wspólnego języka dla wszystkich podręczników i procedur obowiązujących w Organizacji lub w kilku Organizacjach w ramach jednego podmiotu

Urząd Lotnictwa Cywilnego

DZIĘKUJĘ ZA UWAGĘ

Jan Demski
(Główny specjalista, 22 520-73-14, jdemski@ulc.gov.pl)

Anna Czabowska
(Specjalista, 22-520-73-43, aczabowska@ulc.gov.pl)

Sławomir Adam
(Starszy specjalista, 22 520-72-39, sadam@ulc.gov.pl)

1.01.2023