WZÓR DOKUMENTU SYSTEMOWEGO · TQL.PL

Procedura zgłaszania incydentów NIS2

Operacyjny wzór obsługi i zgłaszania incydentów poważnych według art. 11 ustawy o KSC (Dz.U. 2026 poz. 252) i art. 23 dyrektywy (UE) 2022/2555.

Stan prawny i wymagań: 2026-11-15 | Wersja pliku: 2026-11 | Licencja: CC BY 4.0 (tql.pl)

1. Wzór procedury incydentów NIS2 (struktura do wypełnienia)

Dostosuj progi, dyżury i dane pełnomocnika S46 do systemów i usług Twojej firmy.

Nr	Pole dokumentu	Dane Twojej organizacji (do uzupełnienia)	Instrukcja i podstawa
1	Zakres usług i właściwy CSIRT	[Wpisz status KSC (kluczowy/ważny), usługi i właściwy CSIRT]	art. 11 KSC; art. 23 NIS2
2	Kanały zgłoszeń wewnętrznych i dyżur	[Podaj telefon awaryjny i zapasowy adres poza główną domeną]	art. 8 ust. 1 pkt 2 lit. b KSC
3	Kryteria incydentu poważnego	[Określ progi przestoju, skali użytkowników, utraty danych i strat]	art. 11 ust. 1 i 2 KSC
4	Role i pełnomocnik w S46	[Wskaż koordynatora incydentu, osoby w S46 i zastępców]	art. 8 i 11 ustawy o KSC
5	Działania techniczne i zabezpieczenie śladów	[Opisz izolację sieci, zrzut pamięci i zachowanie logów]	art. 21 ust. 2 lit. b NIS2
6	Harmonogram zgłoszeń 24h / 72h / 1 mies.	[Zapisz check-listy wczesnego ostrzeżenia, zgłoszenia i raportu]	art. 11 KSC; art. 23 ust. 4 NIS2
7	Powiadomienie klientów i ocena RODO	[Opisz komunikat dla odbiorców i ścieżkę 72h do Prezesa UODO]	art. 23 ust. 1 i 2 NIS2
8	Rejestr incydentów i wnioski poincydentowe	[Wskaż archiwizację dokumentów i cykliczne przeglądy planu]	art. 8 KSC; ISO 27001 pkt 10.2

2. Przykład wypełnienia: średni zakład produkcyjny (Przykład sp. z o.o.)

Przykład dotyczy fikcyjnego zakładu produkcji maszyn sklasyfikowanego jako podmiot ważny w załączniku nr 2 ustawy o KSC.

Nr	Pole dokumentu	Przykładowy wpis (Przykład sp. z o.o.)
1	Zakres i CSIRT	Przykład sp. z o.o. (podmiot ważny), ERP, sieć OT i poczta; właściwy zespół: CSIRT NASK
2	Kanał awaryjny	Telefon alarmowy dyżurnego IT + komunikator poza domeną firmową na wypadek ataku na AD
3	Progi powagi	Przestój produkcji > 2 h, zaszyfrowanie serwerów, dostęp uprzywilejowany lub wyciek danych

4	Role i S46	Koordynator: kierownik IT (uprawniony w S46); zatwierdzanie: członek zarządu; zastępca: admin sieci
5	Zabezpieczenie śladów	Odłączenie stacji od VLAN bez restartu, wygaszenie sesji VPN, zgranie logów firewall na nośnik WORM
6	Kamienie czasowe	T+0h wpis w dzienniku; T<=24h wczesne ostrzeżenie w S46; T<=72h IoC; T<=30 dni raport końcowy
7	Klienci i RODO	Ocena UODO w 12 h od potwierdzenia wycieku danych; nota do odbiorców B2B przy awarii portalu
8	Przegląd poincydentowy	Analiza przyczyn źródłowych w 7 dni od zamknięcia oraz coroczne ćwiczenie procedury

3. Typowe błędy wynikające z wymagań

Błąd	Konsekwencja	Jak uniknąć / podstawa
Czekanie z raportem 24h na pełną analizę IT	Przekroczenie terminu wczesnego ostrzeżenia.	Wysyłaj sygnalne ostrzeżenie w 24h przed analizą źródłową.
Brak zapasowego kanału komunikacji	Paraliż zgłaszania przy awarii firmowej poczty.	Zapewnij telefon dyżurny i kanał poza siecią lokalną.
Formatowanie serwerów przed zrzutem logów	Utrata śladów IoC dla raportu 72h i miesięcznego.	Najpierw izoluj sieciowo i zabezpiecz pamięć oraz logi.
Brak przygotowanego dostępu do S46	Utrata cennych godzin w trakcie kryzysu.	Wyznacz co najmniej dwie uprawnione osoby z wyprzedzeniem.
Brak wymogów czasowych wobec dostawców IT	Opóźniona informacja o incydencie z chmury.	Wpisz obowiązek alarmu w kilku godzinach do umów SLA.

4. Podstawa wymagań i licencja

Źródła: Dyrektywa (UE) 2022/2555 (NIS2), art. 21 i 23; Ustawa o zmianie ustawy o KSC, Dz.U. 2026 poz. 252 (art. 8 i 11); ISO/IEC 27001:2022.

Uznanie autorstwa CC BY 4.0: Ireneusz Kozera / The Quality of Life (tql.pl). Dokument ma charakter pomocniczy i nie zastępuje analizy własnej organizacji.