WZÓR DOKUMENTU SYSTEMOWEGO · TQL.PL

Rejestr aktywów ISO 27001

Wzór inwentarza informacji i powiązanych aktywów według załącznika A do ISO/IEC 27001:2022 (pkt A.5.9 i A.5.12) oraz wymogów ustawy o KSC.

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

1. Wzór rejestru aktywów ISO 27001 (struktura do wypełnienia)

Uzupełnij pozycje rejestru dla zbiorów informacji, aplikacji, infrastruktury i usług zewnętrznych w zakresie SZBI.

Nr	Pole dokumentu	Dane Twojej organizacji (do uzupełnienia)	Instrukcja i podstawa
1	Identyfikator i kategoria	[Nadaj kod i przypisz grupę: Informacja / System / Sprzęt / Usługa]	ISO 27001 zał. A pkt 5.9
2	Nazwa i opis zasobu	[Wpisz nazwę bazy danych, systemu, klasy urządzeń lub usługi SaaS]	ISO 27001 zał. A pkt 5.9
3	Właściciel biznesowy aktywa	[Wskaż kierownika decydującego o dostępach i klasyfikacji]	ISO 27001 zał. A pkt 5.9
4	Lokalizacja lub dostawca	[Podaj miejsce przechowywania danych lub siedzibę przetwarzającego]	ISO 27001 zał. A pkt 5.9 i 5.21
5	Klasyfikacja poufności	[Przypisz poziom klasyfikacji, np. Jawne / Wewnętrzne / Poufne]	ISO 27001 zał. A pkt 5.12 i 5.13
6	Krytyczność (CIA)	[Oceń wagę Poufności, Integralności i Dostępności oraz docelowe RTO]	ISO 27001 pkt 6.1.2
7	Wymogi prawne lub NDA	[Oznacz RODO, KSC/NIS2, kontrakty poufności z odbiorcami]	ISO 27001 pkt 5.31; art. 8 KSC
8	Data weryfikacji i status	[Wpisz datę przeglądu rejestru i planowany termin kolejnego]	ISO 27001 zał. A pkt 5.9 i 8.14

2. Przykład wypełnienia: dział techniczny i ERP (Przykład sp. z o.o.)

Przykład pokazuje typowy zapis dla zbioru dokumentacji projektowej w fikcyjnym przedsiębiorstwie przemysłowym.

Nr	Pole dokumentu	Przykładowy wpis (Przykład sp. z o.o.)
1	ID i kategoria	AKT-INFO-04 (Informacja / Zbiór projektowy)
2	Nazwa i opis	Baza projektów CAD wyrobów gotowych oraz specyfikacje klientów OEM
3	Właściciel	Kierownik Działu Konstrukcyjno-Technologicznego
4	Lokalizacja / dostawca	Repozytorium PLM w centrum danych

		UE (Frankfurt) + kopia offline poza lokalizacją
5	Klasyfikacja (A.5.12)	Poufne — tajemnica przedsiębiorstwa oraz dokumentacja objęta umowami NDA
6	Krytyczność (CIA)	Poufność: 3/3, Integralność: 3/3, Dostępność: 2/3 (docelowe RTO: 8 godzin)
7	Powiązania prawne	Umowy poufności NDA z klientami; system wspierający objęty analizą ryzyka KSC
8	Weryfikacja	Zweryfikowano 15.11.2026 r.; status: aktywne; następny przegląd: listopad 2027 r.

3. Typowe błędy wynikające z wymagań

Błąd	Konsekwencja	Jak uniknąć / podstawa
Przypisanie wszystkiego wyłącznie do IT	IT nie decyduje o biznesowym dostępie do danych.	Wyznacz właścicieli z działów merytorycznych.
Pominięcie zbiorów danych i chmury SaaS	Szacowanie ryzyka pomija główne wektory wycieku.	Uwzględnij bazy danych, repozytoria i usługi zewnętrzne.
Brak oceny krytyczności CIA aktywów	Nieproporcjonalne nakłady ochronne w firmie.	Powiąż rejestr z oceną ryzyka z pkt 6.1.2.
Brak powiązania z klasyfikacją A.5.12	Personel nie wie, które pliki szyfrować i znakować.	Nadaj jednoznaczną klasę poufności każdemu zbiorowi.
Nieaktualizowanie po wycofaniu lub zakupie IT	Pojawia się shadow IT nieobjęte ochroną.	Wymagaj aktualizacji wykazu przy zakupach i kasacji sprzętu.

4. Podstawa wymagań i licencja

Źródła: ISO/IEC 27001:2022 (załącznik A pkt 5.9, 5.12, 5.13, pkt 6.1.2); Dyrektywa (UE) 2022/2555; Ustawa o KSC (Dz.U. 2026 poz. 252).

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