ITSAILOR, PRZYKŁAD PAKIETU DOWODÓW

Pakiet dowodów: przykład

Jak wygląda pakiet dowodów po wdrożeniu: dane fikcyjne, układ prawdziwy

Wersja 2026-11 · 26.10.2026 · Stan prawny: ustawa o KSC, Dz. U. 2026 poz. 20 ze zm. (poz. 252, 815, 1003, 1206), odczyt 25.10.2026

Przykład zbudowany z danych fikcyjnych. Żaden fragment nie pochodzi z prawdziwego tenanta.

ITSailor · Michal Jatczak, przedsiębiorca zarejestrowany na Malcie, działający pod nazwą handlową ITSailor

Wersja: 2026-11 (przykład) Stan prawny: ustawa o KSC, Dz. U. 2026 poz. 20 ze zm. (poz. 252, 815, 1003, 1206), odczyt 25.10.2026 Przygotował: Michal Jatczak, przedsiębiorca zarejestrowany na Malcie, działający pod nazwą handlową ITSailor

Zanim zaczną Państwo czytać

Ten dokument pokazuje, jak wygląda pakiet dowodów po wdrożeniu, na czterech z kilkudziesięciu kontroli. Wszystkie dane są fikcyjne: firma, tenant, nazwy kont, liczby i daty zostały wymyślone na potrzeby przykładu i nie pochodzą z żadnego prawdziwego tenanta. Fikcyjny podmiot nazywa się „Przykładowa Wytwórnia Elementów sp. z o.o.", ma nieistniejący numer NIP 0000000000 i domenę `przykladowa-wytwornia.example` (domena zarezerwowana do przykładów, RFC 2606). Prawdziwy pakiet ma ten sam układ: streszczenie, rejestr kontroli, macierz Conditional Access, mapa dostępu uprzywilejowanego, rejestr zgód aplikacji, dziennik zmian i weryfikacji, wyjątki i zaległości.

Pakiet dowodów to dokumentacja operacyjna w rozumieniu art. 10 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa. Nie jest certyfikatem, opinią o zgodności ani audytem bezpieczeństwa z art. 15 ustawy. Nie przeprowadzam audytu KSC.

Streszczenie dla zarządu (przykład)

Zlecenie: Przykładowa Wytwórnia Elementów sp. z o.o., podmiot ważny (załącznik 2, produkcja), 180 użytkowników, Microsoft 365 Business Premium z dodatkiem Entra ID P2 dla 6 administratorów. Prace od 3.11.2026 do 14.11.2026, zakres „Tożsamość i dostęp uprzywilejowany".

Obszar	Stan przed (odczyt 3.11.2026)	Stan po (weryfikacja 14.11.2026)	Dowód
MFA administratorów	6 kont administracyjnych, 4 z MFA przez SMS, 2 bez MFA	6 z 6 loguje się kluczem FIDO2 albo passkey	CA03, raport metod uwierzytelniania
MFA użytkowników	Security Defaults, 141 ze 180 osób z MFA (SMS u 97)	polityka CA02 wymuszana, 180 ze 180 z MFA; 158 z passkey w Authenticator, 22 na liście do 1.02.2027	CA02, kampania rejestracji
Konta awaryjne	jedno konto `admin@` ze stałą rolą Global Administrator, hasło w arkuszu	dwa konta awaryjne wyłącznie w chmurze z kluczami FIDO2, wykluczone z każdej polityki, alert i test wykonany	RUNBOOK-02, zapis testu
Dzienniki	audyt ujednolicony włączony, audyt skrzynek wyłączony dla 180 kont	audyt skrzynek włączony dla 180 kont; retencja 180 dni (Audit Standard)	eksport ustawień audytu

Ryzyka szczątkowe: 22 osoby logują się jeszcze kodem SMS (kampania rejestracji passkeys trwa, termin 1.02.2027 od Microsoftu); retencja dzienników 180 dni przy pytaniu o 2 lata z art. 10 ust. 7 (zaległość Z1).

PRZYKŁAD

Rejestr kontroli (cztery wiersze z przykładu)

Kontrola	Pytanie	Art. 8 ust. 1	Stan przed	Stan po	Licencja	Właściciel	Status	Dowód
`ITS-M365-ID-001`	Czy wszystkie konta administratorów muszą przejść MFA przy logowaniu?	pkt 2 lit. l	nie: 2 z 6 bez MFA, 4 przez SMS	tak: CA03 wymaga metody odpornej na phishing, 6 z 6 z FIDO2 lub passkey	Business Premium	Jan Przykładowy, kierownik IT	zaliczone	`CA03-2026-11-10.json`, SHA-256 `3f9c…a1e2`
`ITS-M365-ID-007`	Czy administratorzy i goście mają metodę MFA inną niż SMS lub połączenie głosowe?	pkt 2 lit. l	nie: 4 administratorów tylko SMS, 11 gości tylko SMS	tak: administratorzy FIDO2, goście passkey albo Authenticator	każda edycja Entra ID (rejestracja), P1 (wymuszenie)	Jan Przykładowy	zaliczone	raport metod uwierzytelniania 14.11.2026
`ITS-M365-ID-005`	Czy są co najmniej dwa konta awaryjne wyłącznie w chmurze z passkey lub certyfikatem, stałą rolą Global Administrator, wykluczone z blokujących polityk, z alertem przy użyciu i testem co 90 dni?	pkt 2 lit. f, n	nie: jedno konto, bez wykluczeń, bez alertu	tak: `bg1`, `bg2`, klucze FIDO2 u dwóch różnych osób, alert do dwóch adresatów, test 13.11.2026 zaliczony	Business Premium	Anna Przykładowa, członek zarządu	zaliczone	RUNBOOK-02, zapis testu, reguła alertu `BG-signin`
`ITS-M365-LD-002`	Czy audyt skrzynek pocztowych jest włączony dla wszystkich kont?	pkt 2 lit. g; art. 10 ust. 4	nie: wyłączony dla 180 kont	tak: włączony dla 180 kont	Business Premium	Jan Przykładowy	zaliczone	eksport `Get-MailboxAuditBypass` 14.11.2026

Macierz Conditional Access (wycinek)

Nr	Polityka	Użytkownicy	Przyznanie	Wyjątki i kto je zatwierdził	Tryb i data	Zapis testu
CA02	MFA dla wszystkich użytkowników	wszyscy poza `bg1` i `bg2`	wymagaj MFA	konto skanera `skaner@` (W1), zatwierdził Jan Przykładowy 6.11.2026, przegląd 6.02.2027	report-only od 4.11.2026, wymuszana od 10.11.2026	6 dni report-only: 2 140 logowań, 0 blokad poza skanerem
CA03	MFA dla administratorów przy każdym logowaniu	6 ról uprzywilejowanych	wymagaj metody odpornej na phishing	brak	report-only od 4.11.2026, wymuszana od 10.11.2026	6 dni: 88 logowań administracyjnych, 0 blokad

PRZYKŁAD

Dziennik zmian i weryfikacji (dwa wiersze)

Nr	Data i godzina	Zmiana	Stan przed	Zatwierdził	Okno	Wynik weryfikacji	Ścieżka wycofania	Dowód
4	10.11.2026 18:05	CA02 i CA03 z report-only do wymuszania	report-only od 4.11.2026, 0 blokad użytkowników	Jan Przykładowy, kierownik IT	10.11.2026 18:00 do 20:00	11.11.2026: 412 logowań, 0 blokad użytkowników, 3 oczekiwane blokady skanera przed dodaniem wyjątku	powrót do report-only, natychmiastowy	`CA02-2026-11-10.json`, `CA03-2026-11-10.json`
7	13.11.2026 09:30	test kont awaryjnych	konta utworzone 5.11.2026, nieużywane	Anna Przykładowa, członek zarządu	poza oknem (test)	13.11.2026: logowanie `bg2` kluczem FIDO2 zaliczone, alert dotarł do dwóch adresatów po 3 minutach, rotacja hasła wykonana	nie dotyczy	wpis w dzienniku logowań, zrzut alertu

Wyciąg z dziennika audytu (przykład, dane fikcyjne)

Czas (UTC)	Operacja	Kto	Obiekt	Wynik
2026-11-10T17:08:41Z	Update conditional access policy	adm-jan@przykladowa-wytwornia.example	CA02 (state: enabled)	powodzenie
2026-11-10T17:09:12Z	Update conditional access policy	adm-jan@przykladowa-wytwornia.example	CA03 (state: enabled)	powodzenie
2026-11-13T08:31:05Z	User logged in	bg2@przykladowa-wytwornia.onmicrosoft.com	Microsoft Entra admin center	powodzenie, metoda FIDO2

Wyjątki i zaległości (przykład)

Nr	Rodzaj	Czego dotyczy	Powód	Właściciel	Data przeglądu albo termin
W1	wyjątek	konto `skaner@` poza CA02	urządzenie skanujące bez obsługi nowszych metod uwierzytelniania (modern authentication)	Jan Przykładowy	6.02.2027
Z1	zaległość	retencja dzienników dłuższa niż 180 dni	wymaga Audit Premium (Purview Suite) albo eksportu do Log Analytics	Jan Przykładowy	31.01.2027
Z2	zaległość	22 osoby bez passkey	kampania rejestracji w toku; termin Microsoftu 1.02.2027	Jan Przykładowy	15.01.2027

Przechowywanie

Dokumentację przechowuje Przykładowa Wytwórnia Elementów sp. z o.o. w swoim repozytorium z kontrolą wersji i dostępu (art. 10 ust. 6) co najmniej 2 lata po wycofaniu z użycia (art. 10 ust. 7). Surowe eksporty są w repozytorium klienta; ten pakiet odwołuje się do nich skrótem SHA-256.

Przekazał: Michal Jatczak, 14.11.2026 (przykład). Przyjął: Jan Przykładowy, kierownik IT (przykład).

PRZYKŁAD