ITSAILOR, MAPA KONTROLI

Mapa: art. 8 ust. 1 ustawy o KSC w Microsoft 365 i Entra ID

Art. 8 ust. 1 ustawy o KSC w Microsoft 365 i Entra ID: kontrolka, licencja, zapis dowodu, odniesienie

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

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

---

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

Jak czytać tę mapę

Ustawa o krajowym systemie cyberbezpieczeństwa wymaga od podmiotów kluczowych i ważnych systemu zarządzania bezpieczeństwem informacji (art. 8 ust. 1) i jest neutralna technologicznie: nie nakazuje żadnej klasy systemu ani produktu (FAQ Ministerstwa Cyfryzacji, pytania 3.16 i 3.42, wydanie z października 2026). Ta mapa pokazuje jeden z możliwych sposobów wykonania części technicznej w Microsoft 365, Entra ID, Intune i Microsoft Defender. Nie jest opinią o zgodności, nie zastępuje szacowania ryzyka przez Państwa organizację ani audytu bezpieczeństwa z art. 15 ustawy. Nie przeprowadzam audytu KSC.

Każdy wiersz ma cztery kolumny poza nazwą kontroli:

- **Co w tenancie**: ustawienie albo mechanizm, który wdrażam i którego stan da się odczytać.
- **Licencja**: plan, w którym mechanizm jest dostępny. Fakty licencyjne odczytane na learn.microsoft.com 25.10.2026 (ranga: zobowiązanie dostawcy). Business Premium i E3 zawierają Entra ID P1; PIM, przeglądy dostępu i Conditional Access oparte na ryzyku wymagają Entra ID P2 (E5, E7, Entra Suite albo dodatek P2). Audit Standard przechowuje zapisy 180 dni, Audit Premium rok.
- **Zapis dowodu**: dokument operacyjny w rozumieniu art. 10 ust. 4 ustawy, który zostaje u Państwa w pakiecie dowodów (eksport polityki, raport testu, wyciąg z dziennika).
- **Odniesienie**: publiczny punkt odniesienia z Zestawienia dokumentów normalizacyjnych Ministra Cyfryzacji z 10.09.2026 (art. 45 ust. 3 ustawy; materiał „referencyjny, pomocniczy i informacyjny", nie źródło prawa): CIS Controls v8 z grupami wdrożeniowymi IG1 i IG2 oraz Narodowe Standardy Cyberbezpieczeństwa (NSC 800-53, polskie tłumaczenie NIST SP 800-53). Przypisanie kontroli do liter art. 8 jest moim odczytem tekstu ustawy (ranga: wyliczone).

Identyfikatory kontroli (`ITS-M365-…`) pochodzą z katalogu kontroli ITSailor Tenant Security Baseline, wersja 2026.10; ten sam katalog czyta bezpłatna karta wyniku na itsailor.io/tools i lista kontrolna w pakiecie dowodów.

Art. 8 ust. 1 pkt 1: systematyczne szacowanie ryzyka i zarządzanie nim

Obowiązek organizacyjny, poza tenantem. Wdrożenie dostarcza do niego dane wejściowe: wynik listy kontrolnej (stan przed i po), Microsoft Secure Score z nazwanym właścicielem otwartych działań (`ITS-M365-GV-001`, każdy plan) i listę wyjątków z właścicielem i datą przeglądu. Decyzję o akceptowalnym ryzyku podejmuje Państwa organizacja.

Art. 8 ust. 1 pkt 2: środki techniczne i organizacyjne

lit. a: polityki szacowania ryzyka i bezpieczeństwa systemów

Polityki pisze Państwa organizacja. Z tenanta dostają Państwo eksport każdej polityki Conditional Access w formacie JSON z tabelą celu, zakresu, wyjątków i trybu, żeby polityka dokumentowa i polityka w systemie mówiły to samo.

lit. b: bezpieczeństwo w pozyskiwaniu, rozwijaniu i eksploatacji systemów

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-GV-002`	Baseline security mode w centrum administracyjnym Microsoft 365: ustawienia bez wpływu na użytkowników włączone	każdy plan	zrzut stanu Baseline security mode przed i po	CIS v8 4.1 (IG1); NSC 800-53 CM-6
`ITS-M365-AP-001`	zgoda użytkowników na aplikacje wyłączona albo ograniczona do zweryfikowanych wydawców i uprawnień niskiego ryzyka	każdy plan	eksport ustawień zgody i rejestr zgód aplikacji	CIS v8 2.5, 2.7 (IG2); NSC 800-53 CM-7

lit. c: bezpieczeństwo fizyczne i środowiskowe

Poza tenantem i poza tym wdrożeniem.

lit. d: bezpieczeństwo zasobów ludzkich

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
runbook przyjęcia, zmiany roli i odejścia pracownika	dostęp przez grupy, blokada logowania i unieważnienie sesji w dniu odejścia, konwersja skrzynki, przekazanie plików; zapis, kto i kiedy to wykonał	każdy plan (licencje grupowe: każdy plan; przeglądy dostępu: P2)	zapis cyklu życia konta w dzienniku zmian	CIS v8 5.3, 6.1, 6.2 (IG1); NSC 800-53 PS-4, AC-2

lit. e: bezpieczeństwo łańcucha dostaw

Ocena dostawców jest Państwa obowiązkiem (art. 8 ust. 2). Z mojej strony: karta dostawcy KSC z danymi do wpisu z art. 7 ust. 2 pkt 16 i rejestr zgód aplikacji innych firm w tenancie (`ITS-M365-AP-001`).

lit. f: ciągłość działania i odtwarzanie

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-ID-005`	dwa konta awaryjne (break-glass) wyłącznie w chmurze, z kluczem FIDO2, wykluczone z blokujących polityk Conditional Access, z alertem przy użyciu i testem co 90 dni	każdy plan	runbook kont awaryjnych, zapis testu, wpis w dzienniku logowań	CIS v8 5.2, 6.5 (IG1); NSC 800-53 AC-2(5), CP-2
`ITS-M365-RS-001` , `ITS-M365-RS-002`	chroniona kopia skrzynek, SharePoint i OneDrive poza retencją operacyjną, z określoną granicą awarii i okresem przechowywania	kopia Microsoft 365 Backup płatna od zużycia albo narzędzie innego dostawcy; retencja Purview w każdym planie	zrzut konfiguracji kopii, zakres objętych zasobów	CIS v8 11.2, 11.3 (IG1); NSC 800-53 CP-9
`ITS-M365-RS-003`	test odtworzenia wykonany w ciągu ostatnich 6 miesięcy, ze zmierzonym czasem	jak wyżej	protokół testu odtworzenia	CIS v8 11.5 (IG2); NSC 800-53 CP-4

Plan ciągłości działania i jego testy pozostają dokumentem Państwa organizacji.

lit. g: ciągłe monitorowanie systemów

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-LD-001`	ujednolicony dziennik audytu w Microsoft Purview włączony	każdy plan; Audit Standard 180 dni, Audit Premium rok (E5 albo Purview Suite)	eksport ustawień audytu, próbka zapisu	CIS v8 8.2, 8.5 (IG1); NSC 800-53 AU-2, AU-12
`ITS-M365-LD-002`	audyt skrzynek pocztowych dla wszystkich kont	każdy plan	eksport ustawień audytu skrzynek	CIS v8 8.2 (IG1); NSC 800-53 AU-2
`ITS-M365-LD-003`	opisany proces przeglądu dzienników co najmniej raz w miesiącu	każdy plan	procedura przeglądu i zapis ostatniego przeglądu	CIS v8 8.11 (IG2); NSC 800-53 AU-6
`ITS-M365-EP-002`	Microsoft Defender for Endpoint albo Defender for Business na wszystkich zarządzanych urządzeniach	Business Premium (Defender for Business) albo E5 (Defender for Endpoint P2)	lista urządzeń wdrożonych w Defender	CIS v8 10.1, 13.2 (IG1, IG2); NSC 800-53 SI-4

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-EM-004`, `ITS-M365-EM-005`	polityki Standard albo Strict w Defender for Office 365, Safe Links i Safe Attachments dla wszystkich użytkowników	Business Premium i E5 (MDO P1 lub P2); E3 ma MDO P1 od 1.07.2026	eksport polityk Defender for Office 365	CIS v8 9.6, 9.7 (IG2); NSC 800-53 SI-3, SI-8

Uwaga do retencji: art. 10 ust. 7 ustawy każe przechowywać dokumentację co najmniej 2 lata po wycofaniu z użycia. Czy obejmuje to automatycznie generowane zapisy z art. 10 ust. 4, pozostaje pytaniem do rozstrzygnięcia w Państwa organizacji; przy 180 dniach Audit Standard wdrożenie zapisuje tę lukę w zaległościach i wskazuje eksport dzienników do Log Analytics albo Audit Premium.

lit. h: ocena skuteczności środków

Ocena jest Państwa obowiązkiem. Z tenanta: Secure Score z nazwanym właścicielem (`ITS-M365-GV-001`), runbook wykrywania dryfu konfiguracji i miesięczny przegląd dzienników (`ITS-M365-LD-003`).

lit. i: edukacja i szkolenia personelu

Poza tym wdrożeniem. Pomocniczo: oznaczenie poczty zewnętrznej dla odbiorców (`ITS-M365-EM-006`, każdy plan), które wspiera rozpoznawanie podszyć.

lit. j: cyberhigiena

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-ID-003`	uwierzytelnianie starszymi protokołami (Basic) zablokowane w całym tenancie	Business Premium, E3, E5 (Conditional Access, Entra ID P1)	eksport polityki CA01 i zapis trybu tylko do raportowania	CIS v8 4.8 (IG2); NSC 800-53 IA-2, CM-7
`ITS-M365-EP-003`	aktualizacje Windows wymuszane politykami Intune	Business Premium, E3, E5 (Intune Plan 1)	eksport pierścieni aktualizacji i raport zgodności	CIS v8 7.3, 7.4 (IG1); NSC 800-53 SI-2
`ITS-M365-EP-007`	Windows LAPS zarządza hasłem lokalnego administratora na każdym zarządzanym urządzeniu	Business Premium, E3, E5	eksport polityki LAPS	CIS v8 5.4 (IG1); NSC 800-53 IA-5

lit. k: kryptografia, w tym szyfrowanie

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-EP-004`	BitLocker wymuszony polityką Intune	Business Premium, E3, E5	raport zgodności szyfrowania	CIS v8 3.6 (IG1); NSC 800-53 SC-28
`ITS-M365-DP-001`	etykiety poufności Microsoft Purview skonfigurowane i opublikowane	E5 albo dodatki Purview; podstawowe etykiety w Business Premium	eksport etykiet i polityk publikacji	CIS v8 3.12 (IG2); NSC 800-53 MP-3

lit. l: bezpieczna komunikacja elektroniczna, w tym uwierzytelnianie wieloskładnikowe

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-ID-001`	MFA wymagane dla wszystkich kont administratorów	Business Premium, E3, E5 (Conditional Access)	eksport polityki CA03, raport metod uwierzytelniania	CIS v8 6.5 (IG1); NSC 800-53 IA-2(1)
`ITS-M365-ID-002`	MFA wymagane dla wszystkich użytkowników	Business Premium, E3, E5	eksport polityki CA02	CIS v8 6.3 (IG1); NSC 800-53 IA-2(2)
`ITS-M365-ID-007`	administratorzy i goście mają metodę MFA inną niż SMS i połączenie głosowe; passkeys dla pozostałych przed 1.02.2027, gdy Microsoft wyłącza SMS i głos (zobowiązanie dostawcy, learn.microsoft.com)	rejestracja passkeys w każdej edycji Entra ID; wymuszenie przez Conditional Access wymaga P1	raport metod uwierzytelniania przed i po, zapis kampanii rejestracji	CIS v8 6.4 (IG2); NSC 800-53 IA-2(6)
`ITS-M365-ID-006`	role uprzywilejowane logują się metodą odporną na phishing (passkey, klucz FIDO2, Windows Hello for Business)	Business Premium, E3, E5 (authentication strengths)	eksport polityki CA z wymaganą siłą uwierzytelniania	CIS v8 6.5 (IG1); NSC 800-53 IA-2(6)
`ITS-M365-ID-009`	goście i użytkownicy zewnętrzni muszą przejść MFA	Business Premium, E3, E5	eksport polityki CA05	CIS v8 6.3 (IG1); NSC 800-53 IA-8
`ITS-M365-EM-001`, `ITS-M365-EM-002`, `ITS-M365-EM-003`	DMARC w trybie wymuszania z raportowaniem, DKIM na każdej domenie wysyłającej, jeden rekord SPF w granicy 10 zapytań	każdy plan (ustawienia DNS i Exchange Online)	wynik testu dostarczalności i zrzut rekordów DNS	CIS v8 9.5 (IG2); NSC 800-53 SC-8
`ITS-M365-EM-007`, `ITS-M365-EM-008`	SMTP AUTH wyłączone z nazwanymi wyjątkami; automatyczne przekazywanie na zewnątrz wyłączone	każdy plan	eksport polityk spamu wychodzącego i ustawień skrzynek	CIS v8 9.1, 9.2 (IG1); NSC 800-53 SC-7

lit. m: zarządzanie aktywami

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-EP-001`	urządzenia użytkowników zarejestrowane w Microsoft Intune	Business Premium, E3, E5	wykaz urządzeń z Intune	CIS v8 1.1 (IG1); NSC 800-53 CM-8
`ITS-M365-EP-009`	polityka zgodności dla każdej zarządzanej platformy; urządzenie bez polityki oznaczone jako niezgodne	Business Premium, E3, E5	eksport polityk zgodności	CIS v8 1.1, 4.1 (IG1); NSC 800-53 CM-2

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-EP-006`	zarządzanie urządzeniami mobilnymi dla każdego dostępu mobilnego do poczty i Teams	Business Premium, E3, E5	eksport polityki CA08 i polityk ochrony aplikacji	CIS v8 4.1 (IG1); NSC 800-53 AC-19

lit. n: polityki kontroli dostępu

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
`ITS-M365-PA-001`	role uprzywilejowane przejrzane i ograniczone w ostatnich 90 dniach	każdy plan	mapa dostępu uprzywilejowanego	CIS v8 5.4 (IG1); NSC 800-53 AC-6
`ITS-M365-PA-002`, `ITS-M365-PA-004`	konta administracyjne wyłącznie w chmurze, niefederowane i osobne od kont codziennych	każdy plan	mapa dostępu uprzywilejowanego, lista kont	CIS v8 5.4 (IG1); NSC 800-53 AC-6(5)
`ITS-M365-PA-003`	mniej niż 5 stałych kont Global Administrator	każdy plan	eksport przypisań ról	CIS v8 5.4 (IG1); NSC 800-53 AC-6
`ITS-M365-PA-005`	aktywacja ról na czas zadania w Privileged Identity Management	E5, E7, Entra Suite albo dodatek Entra ID P2	eksport ustawień PIM i historii aktywacji	CIS v8 5.4, 6.8 (IG1, IG2); NSC 800-53 AC-6(1)
`ITS-M365-ID-004`	dostęp gości przeglądany i ograniczony w czasie	każdy plan; przeglądy dostępu wymagają P2	zapis przeglądu gości	CIS v8 5.3, 6.8 (IG1, IG2); NSC 800-53 AC-2(3)
`ITS-M365-CO-001`	udostępnianie zewnętrzne w SharePoint i OneDrive bez linków „dla każdego”	każdy plan	eksport ustawień udostępniania	CIS v8 3.3 (IG1); NSC 800-53 AC-3
`ITS-M365-EP-005`	Conditional Access wymaga urządzenia zgodnego albo dołączonego hybrydowo, co najmniej dla administratorów	Business Premium, E3, E5	eksport polityki CA04	CIS v8 6.4 (IG2); NSC 800-53 AC-17
`ITS-M365-DP-006`	przegląd nadmiernego udostępniania w SharePoint i OneDrive przed wdrożeniem Microsoft 365 Copilot	każdy plan	raport udostępnień z listą do uporządkowania	CIS v8 3.3 (IG1); NSC 800-53 AC-3

Art. 8 ust. 1 pkt 3: zbieranie informacji o zagrożeniach i podatnościach

Źródła organizacyjne: komunikaty CERT Polska (cert.pl), moje.cert.pl i rekomendacje Pełnomocnika Rządu. W tenancie: Threat analytics w Microsoft Defender XDR (E5) i zalecenia Secure Score (każdy plan). Zapis dowodu: lista źródeł z osobą odpowiedzialną za ich przegląd.

Art. 8 ust. 1 pkt 4: zarządzanie incydentami

Kontrola	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
runbook pierwszej godziny	kto co powstrzymuje w Entra ID i Exchange Online, jakie zapisy zabezpieczyć, kto decyduje o zgłoszeniu; zegar z art. 11 ust. 1: wczesne ostrzeżenie do 24 godzin od wykrycia (pkt 4), zgłoszenie do 72 godzin (pkt 4a), raport końcowy do miesiąca od zgłoszenia (pkt 4c), przez S46	każdy plan; izolacja urządzenia wymaga Defender for Business albo Defender for Endpoint	runbook, protokół ćwiczenia, zapis testu	CIS v8 17.1 do 17.4 (IG1); NSC 800-61
runbooki przejęcia konta i phishingu	blokada logowania, unieważnienie sesji, usunięcie obcych metod MFA, reguły skrzynki, ZAP, bloki nadawców	każdy plan; Threat Explorer wymaga MDO P2	zapis działań i wyciąg z dziennika audytu	CIS v8 17.4, 17.7 (IG1, IG2); NSC 800-61

Kwalifikacja zdarzenia jako incydentu poważnego i samo zgłoszenie są decyzją Państwa organizacji według progów z rozporządzenia; wdrożenie dostarcza dane i runbook, nie pełni dyżuru.

Art. 8 ust. 1 pkt 5: środki zapobiegające i ograniczające wpływ incydentów

Litera	Co w tenancie	Licencja	Zapis dowodu	Odniesienie
lit. a: mechanizmy poufności, integralności, dostępności i autentyczności	Conditional Access (powyżej), DLP dla poczty wychodzącej `ITS-M365-DP-002` i dla SharePoint i OneDrive `ITS-M365-DP-003`, retencja Teams i SharePoint `ITS-M365-DP-004`	DLP: E5 albo dodatki Purview; retencja: każdy plan	eksport polityk DLP i retencji	CIS v8 3.4, 3.13 (IG1, IG3); NSC 800-53 SC-8, SI-7
lit. b: regularne aktualizacje oprogramowania	pierścienie aktualizacji Intune `ITS-M365-EP-003`	Business Premium, E3, E5	raport zgodności aktualizacji	CIS v8 7.3 (IG1); NSC 800-53 SI-2
lit. c: ochrona przed nieuprawnioną modyfikacją	PIM `ITS-M365-PA-005`, dziennik audytu `ITS-M365-LD-001`, przegląd dryfu konfiguracji	P2 dla PIM; audyt w każdym planie	historia aktywacji ról, eksport konfiguracji	CIS v8 4.1, 8.2 (IG1); NSC 800-53 CM-3, AU-12
lit. d: niezwłoczne działanie przy podatnościach	zarządzanie podatnościami w Defender `ITS-M365-EP-002`, Secure Score `ITS-M365-GV-001`	Business Premium (Defender for Business) albo E5	raport podatności z datami naprawy	CIS v8 7.1, 7.2 (IG1); NSC 800-53 RA-5

Zastrzeżenia

1. Mapa dotyczy części technicznej systemu zarządzania bezpieczeństwem informacji w zakresie Microsoft 365 i Entra ID. Szacowanie ryzyka, polityki, łańcuch dostaw, plan ciągłości, szkolenia i audyt bezpieczeństwa z art. 15 pozostają po stronie Państwa organizacji.
2. Jedno ustawienie nie wykonuje obowiązku ustawowego. O tym, czy środek jest „proporcjonalny" (art. 8 ust. 1 pkt 2), decyduje Państwa analiza ryzyka.
3. Fakty licencyjne i terminy Microsoft pochodzą z learn.microsoft.com z 25.10.2026 i zmieniają się z wydaniami dostawcy.
4. Przypisanie kontroli do liter art. 8 jest odczytem jednego inżyniera, nie stanowiskiem organu. Poradnik NASK „KSC 2.0" z 29.09.2026 numeruje te same litery inaczej w tabeli 4 i w tekście; mapa cytuje Dziennik Ustaw.

Brief po polsku: itsailor.io/pl/kontakt?source=pl-100. Oferta wyłącznie dla firm. Usług opisanych na tej stronie nie świadczę konsumentom.