

Pakiet Dokumentacji dla ISO 27001

Uwaga: Wdrażanie dokumentacji powinno w miarę możliwości być realizowane w kolejności podanej poniżej. Kolejność wdrażania dokumentacji związanej z Aneks A jest określona w Planie postępowania z ryzykiem.

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiązkowy zgodnie z ISO 27001
0.	Procedura zarządzania dokumentami i rejestrami	ISO/IEC 27001 7.5	
1.	Plan projektu		
2.	Procedura identyfikacji wymagań	ISO/IEC 27001 4.2 oraz A.18.1.1	
2.1.	Załącznik – Lista wymagań prawnych, branżowych, umownych i innych	ISO/IEC 27001 4.2 oraz A.18.1.1	✓*
3.	Zakres SZBI	ISO/IEC 27001 4.3	✓
4.	Polityka bezpieczeństwa informacji	ISO/IEC 27001 5.2 oraz 5.3	✓
5.	Metodyka szacowania i postępowania z ryzykiem	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, oraz 8.3	✓
5.1.	Załącznik 1 – Tabela szacowania ryzyka	ISO/IEC 27001 6.1.2 oraz 8.2	✓
5.2.	Załącznik 2 – Tabela postępowania z ryzykiem	ISO/IEC 27001 6.1.3 oraz 8.3	✓
5.3.	Załącznik 3 – Raport z szacowania i postępowania z ryzykiem	ISO/IEC 27001 8.2 oraz 8.3	✓
6.	Deklaracja stosowania	ISO/IEC 27001 6.1.3 d)	✓
7.	Plan postępowania z ryzykiem	ISO/IEC 27001 6.1.3, 6.2 oraz 8.3	✓
8.	(Aneks A – zabezpieczenia)		

Numer w pakiecie	Nazwa dokumentu	Odnoszące sekcje norm	Obowiązkowy zgodnie z ISO 27001
8. A.6	Polityka użytkowania własnych urządzeń elektronicznych (Polityka BYOD)	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1	
8. A.6	Polityka użytkowania urządzeń mobilnych i telepracy	ISO/IEC 27001 A.6.2 A.11.2.6	
8. A.7	Zobowiązanie do zachowania poufności	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2	✓ *
8. A.7	Zobowiązanie do stosowania polityk i procedur SZBI	ISO/IEC 27001 A.7.1.2	✓ *
8. A.8	Inwentaryzacja aktywów	ISO/IEC 27001 A.8.1.1, A.8.1.2	✓ *
8. A.8	Polityka akceptowalnego użytkowania	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2	✓ *
8. A.8	Polityka klasyfikacji informacji	ISO/IEC 27001 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3	
8. A.9	Polityka kontroli dostępu	ISO/IEC 27001 A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3	✓ *
8. A.9	Polityka zarządzania hasłami (Uwaga: może być częścią Polityki kontroli dostępu)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3	

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001
8. A.10	Polityka stosowania zabezpieczeń kryptograficznych	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5	
8. A.11	Polityka czystego biurka i czystego ekranu (Uwaga: może być częścią Polityki akceptowalnego użytkowania)	ISO/IEC 27001 A.11.2.8, A.11.2.9	
8. A.11	Polityka usuwania i niszczenia informacji (Uwaga: może być częścią Procedur operacyjnych dla systemów teleinformatycznych)	ISO/IEC 27001 A.8.3.2, A.11.2.7	
8. A.11	Procedury pracy w strefach bezpieczeństwa	ISO/IEC 27001 A.11.1.5	
8. A.12	Procedury operacyjne dla systemów teleinformatycznych	ISO/IEC 27001 A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4	✓ *
8. A.12	Polityka zarządzania zmianami (Uwaga: może być częścią Procedur operacyjnych dla systemów teleinformatycznych)	ISO/IEC 27001 A.12.1.2, A.14.2.4	
8. A.12	Polityka zarządzania kopiami zapasowymi (Uwaga: może być częścią Procedur operacyjnych dla systemów teleinformatycznych)	ISO/IEC 27001 A.12.3.1	

Numer w pakiecie	Nazwa dokumentu	Odnoszące sekcje norm	Obowiązkowy zgodnie z ISO 27001
8. A.13	Polityka przekazywania informacji (Uwaga: może być częścią Procedur operacyjnych dla systemów teleinformatycznych)	ISO/IEC 27001 A.13.2.1, A.13.2.2	
8. A.14	Polityka bezpiecznego rozwoju systemów	ISO/IEC 27001 A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1	✓ *
8. A.14	Załącznik – Specyfikacja wymagań dla systemu przetwarzania informacji	ISO/IEC 27001 A.14.1.1	✓ *
8. A.15	Polityka bezpieczeństwa dotycząca dostawców	ISO/IEC 27001 A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	
8. A.15	Załącznik – Klauzule bezpieczeństwa dla dostawców i partnerów	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3	✓ *
8. A.16	Procedura zarządzania incydentami	ISO/IEC 27001 A.7.2.3, A.16.1.1, A.6.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	✓ *
8. A.16	Załącznik – Dziennik incydentów	ISO/IEC 27001 A.16.1.6	
8. A.17	Plan odtworzenia po katastrofie	ISO/IEC 27001 A.17.1.2	✓ *
9.	Plan szkolenia i uświadamiania	ISO/IEC 27001 7.2, 7.3	✓
10.	Procedura audytu wewnętrznego	ISO/IEC 27001 sekcja 9.2	

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001
10.1.	Załącznik 1 – Roczny program audytu wewnętrznego	ISO/IEC 27001 sekcja 9.2	✓
10.2.	Załącznik 2 – Raport z audytu wewnętrznego	ISO/IEC 27001 sekcja 9.2	✓
10.3.	Załącznik 3 – Lista kontrolna audytu wewnętrznego	ISO/IEC 27001 sekcja 9.2	
11.	Protokół z przeglądu dokonanego przez kierownictwo	ISO/IEC 27001 sekcja 9.3	✓
12.	Procedura działań naprawczych	ISO/IEC 27001 sekcja 10.1	
12.1.	Załącznik – Formularz działania naprawczego	ISO/IEC 27001 sekcja 10.1	✓

*Podane dokumenty są obowiązkowe tylko wtedy, jeśli odnośne zabezpieczenia są wskazane do zastosowania w Zakresie SZBI.

Aby zobaczyć, jak wypełniać wymienione wyżej dokumenty, zapoznaj się z:

- 1) Naszymi wideo-szkoleniami <http://advisera.com/27001academy/documentation-tutorials/>
- 2) Naszymi seminariami internetowymi <http://advisera.com/27001academy/webinars/>