
Spis treści

Wstęp	9
Rozdział 1	
Wdrażanie systemu ochrony danych osobowych	
– kolejność działań	11
Od dostosowania zabezpieczeń	14
Przez szkolenie osób upoważnionych	15
Do okresowych sprawdzeń systemu ochrony	17
Rozdział 2	
Wdrażanie adekwatnych zabezpieczeń fizycznych	19
Kontrola dostępu do obszaru przetwarzania	20
Zamki mechaniczne i elektroniczne	21
Monitoring wizyjny i systemy alarmowe	24
Technologia biometryczna	27
Systemy przeciwpożarowe	29
Pozostałe zabezpieczenia pasywne	31
Rozdział 3	
Wdrażanie adekwatnych zabezpieczeń organizacyjnych	35
Polityka kluczy	35
Polityka haseł	37

Polityka czystego biurka	39
Polityka czystego ekranu	40
Polityka czystego druku	41
Procedura korzystania z internetu i poczty elektronicznej	43
Procedura korzystania z urządzeń przenośnych	45
Procedura tworzenia i przechowywania kopii zapasowych	48
Procedura wykonywania przeglądów i konserwacji systemów informatycznych	51
Procedura nadawania upoważnień do przetwarzania danych osobowych	53
Procedura nadawania i odbierania uprawnień w systemach informatycznych	55
Procedura monitorowania systemu informatycznego	57
Procedura alarmowa	59

Rozdział 4

Wdrażanie zabezpieczeń infrastruktury informatycznej i telekomunikacyjnej	63
Zabezpieczenia pomieszczenia serwerowni i sieci informatycznej	63
Alternatywny dostęp do sieci publicznej	67
Alternatywne zasilanie w energię elektryczną	67
System informatyczny centralnie i lokalnie zarządzany	69
Konfiguracja sieci Wi-Fi	71
Zdalny dostęp do zasobów wewnętrznych	72
Zewnętrzne kolokacje – zewnętrzne data center	75
Rejestratory rozmów telefonicznych	78
Rejestratory nagrań wideo	79

Rozdział 5

Wdrażanie narzędzi programowych i środków ochrony baz danych osobowych	84
Systemy operacyjne i ich konfiguracja	85
Konfiguracja poczty elektronicznej	87
Ograniczanie dostępu do sieci publicznej	89
Zapora ogniowa	91
Oprogramowanie antywirusowe	93

Zabezpieczenia stron internetowych	93
Zabezpieczenia usług świadczonych drogą elektroniczną	94

Rozdział 6

Zapoznanie osób upoważnionych z procedurami i zabezpieczeniami	96
Szkolenie stacjonarne	96
Szkolenie w formie e-learningu	99
Testy sprawdzające	101
Minimalny zakres wiedzy osób upoważnionych	103
Różnicowanie zakresu szkoleń	104
Szkolenia stanowiskowe	105

Rozdział 7

Wdrażanie instrukcji alarmowej ochrony danych osobowych	108
Dostępność regulacji wewnętrznych i kontakt z ABI	109
Katalog zagrożeń systemu ochrony danych	110
Identyfikacja incydentów ochrony danych	112

Rozdział 8

Sprawdzenia systemu ochrony danych	113
Korzystanie z narzędzi do dokonywania sprawdzeń	114
Sprawozdania ze sprawdzeń	120
Rekomendacje w zakresie dostosowania	120

Rozdział 9

Nadzór nad podmiotami zewnętrznymi w zakresie przetwarzania danych osobowych	124
Stosowanie list kontrolnych	124
Kontrole bezpośrednie w podmiocie zewnętrznym	126
Postępowanie w przypadku stwierdzenia uchybień	128
Rekomendacje co do ukarania lub zmiany podmiotu zewnętrznego	129

Rozdział 10

Szacowanie ryzyka w systemie ochrony danych osobowych 131

Metodologia szacowania ryzyka 132

Ryzyka zewnętrzne i wewnętrzne 133

Stopniowanie ryzyka 133

Zakończenie 135

Bibliografia 136