


Konrad Gałaj-Emiliańczyk

**Wdrożenie systemu zarządzania
bezpieczeństwem informacji
zgodnie z normą
ISO/IEC 27001:2019**




ODDK Spółka z ograniczoną odpowiedzialnością Spółka komandytowa
Gdańsk 2021

© Copyright by ODDK Spółka z ograniczoną odpowiedzialnością Spółka komandytowa
 Gdańsk 2021


Opracowanie redakcyjne i korekta:

 Jerzy Toczek

Redaktor prowadzący:

 Anna Osipów

Koncepcja i projekt okładki:

 Artur Zdulski

Skład tekstu:

Mariusz Szewczyk

Kopiowanie na dowolnych nośnikach, przedruk, rozpowszechnianie całości lub fragmentów bez pisemnej zgody Wydawcy – ODDK Spółki z ograniczoną odpowiedzialnością Spółka komandytowa – jest zabronione i zagrożone karą pozbawienia wolności do lat 5.

Materiał powielany (kserowany) narusza prawa autorskie!

ISBN 978-83-7804-841-1



Wydawca: ODDK Spółka z ograniczoną odpowiedzialnością Spółka komandytowa
80-317 Gdańsk-Oliwa, ul. Obrońców Westerplatte 32A
www.oddk.pl; e-mail: oddk@oddk.pl; tel./faks 58 554 29 17
BDO 00035465

Spis treści

Wstęp	9
Rozdział 1. Bezpieczeństwo informacji	13
Czym jest bezpieczeństwo informacji?	15
Jaki jest cel zarządzania bezpieczeństwem informacji?	18
Czy warto zarządzać bezpieczeństwem informacji?	21
Jakie zasoby będą potrzebne, by zarządzać bezpieczeństwem informacji?	23
Czy warto starać się o certyfikat ISO/IEC 27001?	25
Rozdział 2. Przygotowanie do wdrożenia SZBI	29
Terminy i definicje – jak je rozumieć?	30
Identyfikacja kontekstu organizacji	33
Planowanie ról i odpowiedzialności	37
Tworzenie dokumentacji SZBI	50
Ciągłe doskonalenie SZBI	55
Rozdział 3. Cele stosowanych zabezpieczeń	59
Polityka bezpieczeństwa	60
Organizacja bezpieczeństwa informacji	62
Bezpieczeństwo zasobów ludzkich	65
Zarządzanie aktywami	68
Kontrola dostępu	74
Kryptografia	79
Bezpieczeństwo fizyczne i środowiskowe	81
Bezpieczna eksploatacja	86
Bezpieczeństwo komunikacji	97
Pozyskiwanie, rozwój i utrzymanie systemów	102
Relacje z dostawcami	106
Zarządzanie incydentami związanymi z bezpieczeństwem informacji	108
Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	111
Zgodność SZBI	114
Rozdział 4. Ryzyko w bezpieczeństwie informacji	121
Inwentaryzacja aktywów informacyjnych	125
Wybór metody przeprowadzania analizy ryzyka	127
Szacowanie ryzyka w bezpieczeństwie informacji	130
Postępowanie z ryzykiem w bezpieczeństwie informacji	132
Ocena skuteczności postępowania z ryzykiem	136

Rozdział 5. Wdrożenie SZBI	139
Dostosowanie zabezpieczeń	140
Zatwierdzenie i ogłoszenie dokumentacji SZBI	151
Szkolenie personelu z bezpieczeństwa informacji	153
Zapewnienie bezpieczeństwa informacji z dostawcami	154
Deklaracja stosowania	155
Rozdział 6. Utrzymanie SZBI	159
Zarządzanie incydentami bezpieczeństwa informacji	160
Najczęściej występujące incydenty	160
Rejestrowanie i raportowanie incydentów bezpieczeństwa informacji	163
Testowanie zabezpieczeń	164
Raportowanie wyników testów	165
Rozdział 7. Audyt wewnętrzny SZBI	167
Kompetencje audytorów wewnętrznych	168
Program audytu wewnętrznego	168
Planowanie audytów	169
Raportowanie wyników audytu	172
Działania korekcyjne i korygujące	173
Rozdział 8. SZBI a zgodność z prawem	177
SZBI a zgodność z RODO	178
SZBI a ochrona informacji niejawnych	179
SZBI a Krajowe Ramy Interoperacyjności (KRI)	180
SZBI a Krajowy System Cyberbezpieczeństwa (KSC)	182
Praktyka implementacji przepisów prawa do SZBI	184
Rozdział 9. Wyzwania dla bezpieczeństwa informacji	187
Nowe technologie a stare przyzwyczajenia	188
Poziom świadomości personelu a socjotechniki	190
Internet rzeczy (IoT) a standardowe zabezpieczenia	191
Metody działania i tendencje w cyberprzestępczości	192
Kierunki rozwoju bezpieczeństwa informacji	194
Rozdział 10. Doskonalenie SZBI	197
Rodzina norm ISO 27000	198
Bezpieczeństwo informacji a inne systemy zarządzania	199
Przegląd SZBI	201
Planowanie doskonalenia SZBI	203
Ciągłe doskonalenie SZBI w praktyce	204
Podsumowanie	207
Wykaz aktów prawnych i norm	209
Spis rysunków	211