

Spis treści

O autorze	5
Wstęp	7
Zezwolenie	9
Od autora	11
Podstawowe założenia polityki bezpieczeństwa informacji	13
Czym jest informacja	13
Gdzie przechowujemy informacje	14
Informacja w świetle regulacji prawnych	15
Zasady audytu	15
Norma ISO/IEC TR 13335	19
Zarządzanie bezpieczeństwem informacji	23
Polityka bezpieczeństwa informacji	23
Co powinna zawierać polityka bezpieczeństwa informacji	24
Czego nie powinna zawierać polityka bezpieczeństwa informacji	25
Utworzenie infrastruktury bezpieczeństwa informacji	25
Odpowiedzialność oraz kompetencje w systemie bezpieczeństwa informacji	26
Autoryzacja urządzeń do przetwarzania informacji	26
Doradztwo specjalistyczne w zakresie bezpieczeństwa informacji	27
Współpraca między organizacjami	28
Niezależne przeglądy stanu bezpieczeństwa informacji	28
Zabezpieczenie przed dostępem osób trzecich	29
Zlecenie przetwarzania danych firmom zewnętrznym	33

Klasyfikacja i kontrola aktywów	35
Rozliczanie aktywów	35
Klasyfikacja informacji	37
Bezpieczeństwo osobowe	39
Bezpieczeństwo informacji przy określaniu obowiązków i w zarządzaniu zasobami ludzkimi	39
Szkolenie użytkowników	43
Reagowanie na naruszenia bezpieczeństwa i niewłaściwe funkcjonowanie systemu	44
Bezpieczeństwo fizyczne i środowiskowe	47
Fizyczny obwód zabezpieczający	48
Zabezpieczenie sprzętu	54
Ogólne zabezpieczenia	59
Zarządzanie systemami informatycznymi i sieciami komputerowymi	63
Procedury eksploatacyjne oraz okres odpowiedzialności	63
Planowanie i odbiór systemu	67
Ochrona przed szkodliwym oprogramowaniem	69
Procedury wewnętrzne	71
Zarządzanie sieciami	73
Postępowanie z nośnikami i ich bezpieczeństwo	74
Wymiana danych i oprogramowania	77
Kontrola dostępu do systemu	85
Potrzeby biznesowe związane z dostępem do informacji	85
Zarządzanie dostępem użytkowników	86
Zakres odpowiedzialności użytkowników	89
Kontrola dostępu do sieci	91
Kontrola dostępu do systemów operacyjnych	94
Kontrola dostępu do aplikacji	97
Monitorowanie dostępu do systemu i jego wykorzystywania	98
Komputery przenośne i praca zdalna	100
Zabezpieczenia kryptograficzne	103
Zarządzanie ciągłością działania organizacji w sytuacji krytycznej	105
Zgodność	111
Przegląd polityki bezpieczeństwa informacji i zgodności technicznej	114
Skorowidz	117