					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P02					Tytuł dokumentu: **Polityka ról i odpowiedzialności w zakresie ładu zarządczego**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 5.3; Załącznik A, środek kontrolny 5	
ISO/IEC 27002:2022	Środek kontrolny 5	
NIST SP 800-53 Rev.5	PL-1 do PL-4, PM-1 do PM-13	
RODO	Artykuły 5(1)(f), 24, 37	
Dyrektywa NIS2	Artykuł 21(2)(a)	
Rozporządzenie DORA	Artykuł 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Cel

1.1 Niniejsza polityka określa model ładu zarządczego, role organizacyjne oraz odpowiedzialności wymagane do funkcjonowania skutecznego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

1.2 Ustanawia jasne linie odpowiedzialności, uprawnienia decyzyjne oraz ścieżki eskalacji w celu zapewnienia uwzględnienia bezpieczeństwa informacji na wszystkich poziomach organizacji oraz jego zgodności ze strategicznymi celami biznesowymi.

1.3 Polityka wdraża wymagania normy ISO/IEC 27001:2022, klauzuli 5.3 oraz środka kontrolnego A.5.2, zapewniając, że odpowiedzialności za działania związane z bezpieczeństwem są jednoznacznie przypisane, udokumentowane, zakomunikowane i okresowo poddawane przeglądowi.

1.4 Niniejsza polityka stanowi również podstawę zintegrowanego ładu zarządczego z innymi obszarami, takimi jak zarządzanie ryzykiem, zgodność, operacje IT oraz funkcje prawne.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich osób i podmiotów zaangażowanych w zarządzanie, realizację oraz nadzór nad bezpieczeństwem informacji w granicach zakresu SZBI. Obejmuje to:

2.1.1 kadrę zarządzającą, najwyższe kierownictwo oraz członków zarządu

2.1.2 menedżerów SZBI, Dyrektora ds. Bezpieczeństwa Informacji (CISO) oraz właścicieli środków kontrolnych

2.1.3 właścicieli procesów i aktywów

2.1.4 wykonawców oraz dostawców usług zewnętrznych, którym powierzono odpowiedzialności w zakresie bezpieczeństwa

2.2 Obejmuje ona zarówno funkcje wewnętrzne, jak i realizowane przez podmioty zewnętrzne (np. zewnętrzny SOC, administratorów platform chmurowych), jeżeli role w zakresie ładu zarządczego zostały formalnie przypisane lub określone umownie.

2.3 Polityka ma również zastosowanie do jednostek organizacyjnych, działów i zespołów projektowych, które zarządzają aktywami, systemami lub usługami istotnymi z perspektywy bezpieczeństwa albo wywierają na nie wpływ.

3. Cele

3.1 Zapewnienie, że role i odpowiedzialności w zakresie bezpieczeństwa informacji są formalnie zdefiniowane, przypisane, zakomunikowane i udokumentowane.

3.2 Utrzymanie modelu ładu zarządczego, który zapewnia rozdzielenie obowiązków, eliminuje konflikty interesów oraz umożliwia eskalację nierozwiązanych kwestii związanych z bezpieczeństwem.

3.3 Zapewnienie, że odpowiedzialność i uprawnienia decyzyjne w zakresie bezpieczeństwa są rozdzielone zgodnie z wpływem biznesowym i strukturą organizacyjną.

3.4 Ustanowienie ram zarządzania delegowaniem uprawnień, zmianami ról oraz przeglądem przypisanych odpowiedzialności.

3.5 Zapewnienie interesariuszom — w tym organom regulacyjnym, audytorom i klientom — możliwości wykazania, że bezpieczeństwo informacji jest nadzorowane skutecznie i zgodnie z mającymi zastosowanie normami.

4. Role i odpowiedzialności

4.1 kadra zarządzająca (najwyższe kierownictwo)

4.1.1 Zapewnia nadzór strategiczny, przydziela zasoby oraz dba o zgodność między celami SZBI a celami biznesowymi.

4.1.2 Zatwierdza kluczową dokumentację SZBI, w tym Politykę bezpieczeństwa informacji, plany postępowania z ryzykiem oraz decyzje dotyczące działań naprawczych po audycie.

4.1.3 Uczestniczy w przeglądach zarządzania SZBI i eskaluje decyzje wymagające zatwierdzenia przez zarząd.

4.1.4 Wspiera kulturę bezpieczeństwa i promuje przestrzeganie zasad ładu zarządczego bezpieczeństwa w całej organizacji.

4.2 Komitet Sterujący ds. Bezpieczeństwa Informacji (ISSC)

4.2.1 Pełni funkcję międzyobszarowego organu ładu zarządczego sprawującego nadzór nad SZBI.

4.2.2 Dokonuje przeglądu profilu ryzyka, skuteczności środków kontrolnych, ustaleń audytowych oraz strategicznych inicjatyw bezpieczeństwa.

4.2.3 Ułatwia koordynację między działami (np. IT, prawnym i zgodności, zasobów ludzkich (HR), zarządzania ryzykiem, zgodności, operacji).

4.2.4 Zatwierdza progi eskalacji, alokację budżetu oraz zmiany polityk wymagające zaangażowania kadry zarządzającej.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wymagania dotyczące przeglądu i aktualizacji

9.1 Harmonogram przeglądu

9.1.1 Niniejsza polityka podlega przeglądowi co najmniej raz w roku lub w przypadku wystąpienia:

9.1.1.1 zmian w strukturze organizacyjnej lub składzie kadry zarządzającej

9.1.1.2 rozszerzenia lub ponownego zdefiniowania zakresu SZBI

9.1.1.3 zmian regulacyjnych wpływających na przypisanie ról lub nadzór

9.1.1.4 istotnych ustaleń audytowych lub incydentów związanych z nieskutecznością ładu zarządczego

9.2 Proces przeglądu i zatwierdzania

9.2.1 Menedżer Systemu Zarządzania Bezpieczeństwem Informacji inicjuje i prowadzi proces przeglądu, w tym zbieranie informacji od interesariuszy i informacji zwrotnych z audytu.

9.2.2 Proponowane aktualizacje podlegają przeglądowi przez ISSC i formalnemu zatwierdzeniu przez kadrę zarządzającą.

9.2.3 Każda wersja musi być ewidencjonowana w Rejestrze dokumentów SZBI i zawierać następujące metadane:

9.2.3.1 identyfikator polityki i tytuł

9.2.3.2 numer wersji i podsumowanie zmian

9.2.3.3 data wejścia w życie i data następnego przeglądu

9.2.3.4 właściciel polityki i zatwierdzający

9.2.3.5 poziom klasyfikacji dokumentu

9.2.3.6 historia przechowywania i archiwizacji

10. Powiązane polityki i odniesienia

10.1 Niniejszą politykę należy interpretować łącznie z następującymi politykami:

10.1.1 P1 – P01 Polityka bezpieczeństwa informacji: ustanawia ogólny program bezpieczeństwa i określa odpowiedzialność kierownictwa za zatwierdzenie polityki oraz nadzór strategiczny.

10.1.2 P5 – P05 Polityka zarządzania zmianą: zapewnia, że zmiany w strukturach ładu zarządczego, rolach lub odpowiedzialnościach podlegają udokumentowanemu zatwierdzeniu i przeglądowi ryzyka.

10.1.3 P6 – Polityka zarządzania ryzykiem: identyfikuje ryzyka ładu zarządczego wynikające z konfliktów ról, nieprzypisanych obowiązków lub braku eskalacji oraz określa sposób postępowania z nimi.

10.1.4 P7 – Polityka wdrażania i zakończenia współpracy: zapewnia stosowanie procesów przypisywania i cofania uprawnień dostępu podczas zmian w cyklu życia personelu.

10.1.5 P33 – Polityka monitorowania audytu i zgodności: wspiera niezależny przegląd skuteczności ładu zarządczego i wymaga wdrażania działań korygujących w przypadku niezgodności.

10.2 Polityki te łącznie wspierają jednolite i egzekwowalne ramy ładu zarządczego SZBI.

11. Normy i modele odniesienia

11.1 Niniejsza polityka jest zgodna z uznanymi na świecie normami i modelami dotyczącymi ładu zarządczego bezpieczeństwa informacji oraz odpowiedzialności za role. Zapewnia możliwość prześledzenia wymagań regulacyjnych i certyfikacyjnych oraz wspiera obronną strukturę SZBI.

11.2 ISO/IEC 27001

11.2.1 Klauzula 5.3 – Role organizacyjne, odpowiedzialności i uprawnienia: Niniejsza polityka spełnia wymaganie, aby role istotne dla bezpieczeństwa informacji były jednoznacznie przypisane, zakomunikowane i udokumentowane.

11.2.2 Klauzula 9.3 – Przegląd zarządzania: Niniejsza polityka zapewnia nadzór kadry zarządzającej nad rolami SZBI i ładem zarządczym poprzez kwartalne i roczne przeglądy.

11.2.3 Załącznik A, środek kontrolny 5.2 – Role i odpowiedzialności w zakresie bezpieczeństwa informacji: Definiuje role na poziomie technicznym, operacyjnym i strategicznym, aby zapewnić rozdzielenie obowiązków, własność ryzyka i możliwą do prześledzenia odpowiedzialność.

11.3 ISO/IEC 27002:2022 – Środek kontrolny 5

11.3.1 Zawiera wytyczne wdrożeniowe dotyczące przypisywania odpowiedzialności za bezpieczeństwo informacji w całej organizacji. Niniejsza polityka przyjmuje te wytyczne poprzez określenie typów ról, zasad delegowania, procedur eskalacji i mechanizmów przeglądu.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 do PL-4: Wskazują potrzebę formalnej dokumentacji planistycznej, w tym polityk definiujących ład zarządczy i przypisujących odpowiedzialności w zakresie bezpieczeństwa.

11.4.2 PM-1 (Plan programu bezpieczeństwa informacji) i PM-2 (Starszy specjalista ds. bezpieczeństwa informacji): Znajdują odzwierciedlenie w niniejszej polityce poprzez przypisanie roli CISO/Menedżera Systemu Zarządzania Bezpieczeństwem Informacji oraz formalnych ról ładu zarządczego.

11.4.3 PM-5 do PM-13: Niniejsza polityka spełnia wymagania dotyczące dokumentowania ról, ról związanych z ryzykiem w skali całego przedsiębiorstwa, nadzoru nad zarządzaniem konfiguracją oraz integracji z funkcjami misyjnymi i biznesowymi.

11.5 RODO (2016/679)

11.5.1 Artykuł 5(1)(f): Wymaga ochrony danych osobowych przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem. Niniejsza polityka zapewnia jednoznaczne wyznaczenie i monitorowanie osób odpowiedzialnych za ochronę danych.

11.5.2 Artykuł 24: Wymaga zastosowania odpowiednich zabezpieczeń organizacyjnych, w tym struktur ładu zarządczego.

11.5.3 Artykuł 37: Wymaga wyznaczenia inspektora ochrony danych (IOD), co musi znaleźć odzwierciedlenie w ramach ładu zarządczego organizacji oraz w rejestrze odpowiedzialności.

11.6 Dyrektywa UE NIS2 (2022/2555)

11.6.1 Artykuł 21(2)(a): Nakłada obowiązek wdrożenia polityk dotyczących analizy ryzyka i bezpieczeństwa systemów informacyjnych, w tym odpowiedzialności właściwych dla poszczególnych ról. Niniejsza polityka definiuje takie role oraz mechanizmy ich nadzoru.

11.7 Rozporządzenie DORA (2022/2554)

11.7.1 Artykuł 5 – Ramy zarządzania i kontroli wewnętrznej: Wymaga formalnego przypisania odpowiedzialności za zarządzanie ryzykiem ICT, ról decyzyjnych oraz kanałów raportowania. Niniejsza polityka stanowi podstawę ładu zarządczego ról związanych z bezpieczeństwem w środowiskach ICT.

11.8 COBIT 2019

11.8.1 EDM01 – Ustanowienie ram ładu zarządczego: Niniejsza polityka zapewnia, że SZBI posiada jasno zdefiniowaną strukturę ładu zarządczego zgodną z potrzebami organizacji.

11.8.2 EDM02 – Zapewnienie realizacji korzyści: Łączy działania bezpieczeństwa oparte na rolach z celami strategicznymi i operacyjnymi, zapewniając odpowiedzialność i mierzalne rezultaty.

11.8.3 APO01 – Ramy zarządzania I&T oraz APO12 – Zarządzanie ryzykiem: Niniejsza polityka wspiera uporządkowane zarządzanie rolami w zakresie bezpieczeństwa informacji w szerszych ramach ładu IT i zarządzania ryzykiem.

11.8.4 MEA01 – Monitorowanie, ocena i analiza wydajności: Wbudowuje mechanizmy przeglądu służące weryfikacji, że role ładu zarządczego są skuteczne, aktualne i stosowane.