					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P02S					Tytuł dokumentu: **Polityka ról i odpowiedzialności w zakresie nadzoru nad bezpieczeństwem**							
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	
ISO/IEC 27002:2022	Środki kontroli: 5.2, 5.3, 5.4	
RODO	Artykuły 5 ust. 2, 32	

1. Cel

1.1 Niniejsza polityka określa sposób przypisywania, delegowania i zarządzania odpowiedzialnościami w obszarze nadzoru nad bezpieczeństwem informacji w organizacji, w celu zapewnienia zgodności z ISO/IEC 27001:2022 oraz innymi mającymi zastosowanie wymogami regulacyjnymi.

1.2 Zapewnia rozliczalność na każdym poziomie organizacji oraz wspiera skuteczność operacyjną poprzez jednoznaczne określenie odpowiedzialności za każdą funkcję związaną z bezpieczeństwem.

1.3 Polityka wspiera gotowość audytową oraz buduje zaufanie klientów poprzez wykazanie formalnego nadzoru nad bezpieczeństwem, również w organizacjach dysponujących ograniczonym personelem technicznym lub korzystających z outsourcingu IT.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich osób korzystających z systemów informatycznych organizacji lub przetwarzających jej dane, w tym:

2.1.1 właścicieli biznesowych i Dyrektora Generalnego

2.1.2 pracowników i współpracowników

2.1.3 zewnętrznych dostawców usług IT lub konsultantów

2.2 Obejmuje wszystkie systemy, środowiska i usługi wykorzystywane do przetwarzania, przesyłania lub przechowywania informacji biznesowych lub informacji klientów, w tym:

2.2.1 infrastrukturę IT w biurze oraz urządzenia wykorzystywane do pracy zdalnej

2.2.2 platformy chmurowe oraz usługi poczty elektronicznej

2.2.3 dokumentację papierową oraz dyski współdzielone

2.3 Zakres obejmuje zarówno działania realizowane wewnętrznie, jak i usługi outsourcowane związane z nadzorem nad bezpieczeństwem informacji.

3. Cele

3.1 Ustanowienie jednoznacznej rozliczalności za wszystkie obowiązki związane z bezpieczeństwem, w tym zarządzanie politykami, kontrolę dostępu, obsługę incydentów i monitorowanie.

3.2 Zapewnienie skutecznego rozdziału obowiązków w celu ograniczenia konfliktu interesów lub ryzyka nadużyć.

3.3 Zapewnienie, że zadania i role związane z bezpieczeństwem są jednoznacznie udokumentowane i regularnie przeglądane.

3.4 Umożliwienie podejmowania świadomych decyzji, eskalacji oraz nadzoru nad ryzykami IT i bezpieczeństwa informacji.

3.5 Wsparcie certyfikacji ISO/IEC 27001:2022 oraz budowanie zaufania klientów, partnerów i audytorów.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny / właściciel biznesowy

4.1.1 Ponosi pełną odpowiedzialność za wdrożenie niniejszej polityki oraz nadzór nad jej stosowaniem.

4.1.2 Zatwierdza wszystkie role bezpieczeństwa, zakresy odpowiedzialności oraz decyzje o delegowaniu.

4.1.3 Monitoruje zgodność oraz podejmuje ostateczne decyzje dotyczące odstępstw od polityki i eskalacji.

4.2 Wyznaczony koordynator ds. bezpieczeństwa (jeżeli został powołany)

4.2.1 Funkcję tę może pełnić pracownik lub zaufany konsultant.

4.2.2 W mikroprzedsiębiorstwie rolę tę może pełnić Dyrektor Generalny lub podmiot zewnętrzny.

4.2.3 Wspiera bieżące stosowanie kontroli dostępu, reagowanie na incydenty oraz realizację podstawowych technicznych zadań z zakresu bezpieczeństwa.

4.2.4 Raportuje bezpośrednio do Dyrektora Generalnego wszelkie kwestie lub ryzyka związane z bezpieczeństwem.

[... 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 Coroczny przegląd

9.1.1 Niniejsza polityka musi być poddawana przeglądowi przez Dyrektora Generalnego co 12 miesięcy w celu zapewnienia, że nadal odzwierciedla obowiązki prawne, potrzeby operacyjne oraz wymagania certyfikacyjne ISO/IEC 27001.

9.2 Przeglądy doraźne

9.2.1 Przeglądy muszą być również przeprowadzane, gdy:

9.2.1.1 zachodzą istotne zmiany organizacyjne

9.2.1.2 wdrażany jest nowy dostawca

9.2.1.3 wystąpi poważny incydent bezpieczeństwa

9.2.1.4 zostaną zaktualizowane regulacje, takie jak RODO, dyrektywa NIS2 lub rozporządzenie DORA

9.3 Kontrola wersji i dokumentacja

9.3.1 Każdy przegląd musi obejmować:

9.3.1.1 datę przeglądu

9.3.1.2 podsumowanie zmian

9.3.1.3 podpis Dyrektora Generalnego lub udokumentowaną akceptację

9.3.1.4 zarchiwizowane wcześniejsze wersje na potrzeby odniesienia audytowego

9.4 Komunikowanie zmian

9.4.1 Wszystkie aktualizacje polityki muszą być niezwłocznie komunikowane personelowi i dostawcom za pośrednictwem poczty elektronicznej, portali wewnętrznych lub formalnych komunikatów.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka powinna być wdrażana łącznie z następującymi politykami SME, aby zapewnić pełną skuteczność:

10.1.1 P4S – Polityka kontroli dostępu: określa sposób nadawania, zarządzania i cofania dostępu, bezpośrednio w powiązaniu z przypisanymi rolami i nadzorem.

10.1.2 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: wzmacnia odpowiedzialności i oczekiwania właściwe dla danej roli.

10.1.3 P17S – Polityka ochrony danych i prywatności: określa obowiązki prawne wynikające z RODO, przypisane do ról zdefiniowanych w niniejszej polityce nadzoru.

10.1.4 P30S – Polityka reagowania na incydenty: wymaga zdefiniowania odpowiedzialności za zgłaszanie, eskalację i obsługę incydentów.

10.2 Łącznie polityki te zapewniają spójne stosowanie wymagań, wewnętrzną rozliczalność i zgodność z wymaganiami zewnętrznymi.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 5.3 – role organizacyjne, odpowiedzialności i uprawnienia: wymaga jednoznacznego przypisania ról oraz wsparcia ze strony najwyższego kierownictwa.

11.2 ISO/IEC 27002

11.2.1 Środki kontroli 5.2–5.4: wymagają jednoznacznego dokumentowania ról w zakresie bezpieczeństwa informacji, rozdziału obowiązków oraz nadzoru kierowniczego.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PM-1: ustanawia nadrzędny program bezpieczeństwa informacji z określonymi odpowiedzialnościami.

11.3.2 PL-1 do PL-4: wymagają zabezpieczeń planistycznych, w tym opracowania polityk i udokumentowanych przypisań ról.

11.3.3 CA-1: wymaga zdefiniowanych ról w zakresie oceny i autoryzacji.

11.3.4 AC-1: wiąże kontrolę dostępu opartą na rolach (RBAC) z przypisanymi odpowiedzialnościami w ramach nadzoru.

11.4 RODO

11.4.1 Artykuł 5 ust. 2 – rozliczalność: wymaga, aby organizacje wykazywały zgodność poprzez role i odpowiedzialności.

11.4.2 Artykuł 32 – bezpieczeństwo przetwarzania: podkreśla potrzebę jednoznacznego przypisania obowiązków w celu ochrony danych osobowych.

11.5 Dyrektywa UE NIS2

11.5.1 Artykuł 21 ust. 2 lit. a: wymaga struktur nadzorczych obejmujących sformalizowane role do zarządzania cyberryzykiem i incydentami.

11.6 Rozporządzenie DORA

11.6.1 Artykuły 9 i 10: wymagają, aby podmioty finansowe jednoznacznie przypisywały i nadzorowały odpowiedzialności związane z ICT i bezpieczeństwem.

11.7 COBIT 2019

11.7.1 EDM03 – Ensure Risk Optimization: wymaga dobrze zdefiniowanych ról i ścieżek eskalacji w zarządzaniu ryzykiem bezpieczeństwa.

11.7.2 APO13 – Manage Security: przypisuje strategiczne i operacyjne obowiązki bezpieczeństwa do osób i ról.

11.7.3 DSS05 – Zarządzanie usługami bezpieczeństwa: wymaga struktury i możliwości prześledzenia odpowiedzialności za zewnętrzne i wewnętrzne usługi bezpieczeństwa.