					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P33					Tytuł dokumentu: **Polityka audytu i monitorowania zgodności**							
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	Klauzule 9.2, 9.3, 10	
ISO/IEC 27002:2022	Zabezpieczenia 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
RODO	Artykuły 24, 32, 33	
Dyrektywa NIS2	Artykuły 21(2)(g), 27	
Rozporządzenie DORA	Artykuły 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Cel

1.1 Celem niniejszej polityki jest ustanowienie programu audytu i monitorowania zgodności w organizacji oraz określenie zasad jego nadzoru w celu:

1.1.1 potwierdzenia skuteczności zabezpieczeń bezpieczeństwa i prywatności

1.1.2 zapewnienia zgodności z mającymi zastosowanie normami, przepisami prawa i zobowiązaniami umownymi

1.1.3 terminowego wykrywania niezgodności, nieskuteczności i ryzyk w obszarze zgodności

1.1.4 wspierania ciągłego doskonalenia oraz gotowości do certyfikacji, ocen i przeglądów regulacyjnych

1.2 Niniejsza polityka wspiera integralność i dojrzałość Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) poprzez wdrożenie ustrukturyzowanych, opartych na ryzyku i dowodach praktyk audytowych oraz monitorowania.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich:

2.1.1 wewnętrznych jednostek organizacyjnych, funkcji i działów

2.1.2 lokalizacji fizycznych, środowisk chmury obliczeniowej, platform SaaS i usług realizowanych w outsourcingu

2.1.3 systemów informatycznych, aplikacji, infrastruktury i aktywów informacyjnych objętych SZBI

2.1.4 pracowników, współpracowników i dostawców zewnętrznych, na których ciążą obowiązki audytowe lub obowiązki w zakresie zgodności

2.2 Polityka obejmuje:

2.2.1 audyty wewnętrzne

2.2.2 audyty zewnętrzne i certyfikacyjne

2.2.3 techniczne monitorowanie zgodności

2.2.4 audyty dostawców i podmiotów trzecich

2.2.5 działania korygujące i zapobiegawcze (CAPA)

2.2.6 metryki, pulpity oraz procesy raportowania

2.3 Ma ona zastosowanie do wszystkich właściwych ram i wymagań, którym podlega organizacja, w tym między innymi ISO/IEC 27001, RODO, NIS2, DORA i SOC 2.

3. Cele

3.1 Weryfikacja adekwatności i skuteczności wdrożonych zabezpieczeń, polityk i procedur w całym SZBI oraz środowiskach powiązanych.

3.2 Identyfikowanie i usuwanie wszelkich słabości, niezgodności lub luk w zgodności, zanim doprowadzą do incydentów lub naruszeń.

3.3 Zapewnienie stałej gotowości do wewnętrznych przeglądów ładu organizacyjnego, audytów zewnętrznych i niezależnych certyfikacji.

3.4 Tworzenie możliwych do obrony dowodów oraz ścieżek audytowych na potrzeby zapytań organów regulacyjnych, postępowań prawnych lub wniosków klientów o zapewnienie.

3.5 Integracja wyników audytów z szerszymi działaniami organizacji w zakresie zarządzania ryzykiem, metryk bezpieczeństwa oraz ciągłego doskonalenia.

4. Role i obowiązki

4.1 Osoba odpowiedzialna za audyt wewnętrzny / Menedżer ds. zgodności

4.1.1 planuje, harmonogramuje i realizuje audyty wewnętrzne zgodnie z priorytetami wynikającymi z ryzyka.

4.1.2 prowadzi Rejestr audytów, koordynuje działania audytowe i nadzoruje realizację działań korygujących.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO)

4.2.1 zapewnia, że zakres audytu obejmuje wszystkie odpowiednie elementy SZBI oraz zabezpieczenia z Załącznika A.

4.2.2 sprawuje nadzór nad weryfikacją CAPA i integruje wyniki audytów z programem bezpieczeństwa.

[... 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 Niniejsza polityka musi być poddawana przeglądowi co najmniej raz w roku przez Menedżera ds. zgodności i CISO albo wcześniej, w odpowiedzi na:

9.1.1 zmiany wymagań regulacyjnych, umownych lub certyfikacyjnych

9.1.2 istotne ustalenia audytowe lub powtarzające się nieskuteczności zabezpieczeń

9.1.3 restrukturyzację organizacji lub zmiany systemu GRC

9.1.4 rekomendacje audytora zewnętrznego lub informacje zwrotne od organu regulacyjnego

9.2 W ramach przeglądu należy ocenić:

9.2.1 metodykę planowania audytów i ich częstotliwość

9.2.2 zmiany zakresu SZBI lub infrastruktury

9.2.3 aktualizacje katalogu zabezpieczeń lub rejestru wymagań prawnych

9.2.4 spójność i jakość dowodów audytowych oraz procesów CAPA

9.3 Wszystkie zmiany polityki muszą być:

9.3.1 udokumentowane w repozytorium objętym kontrolą wersji

9.3.2 zatwierdzone przez kierownictwo wykonawcze

9.3.3 przekazane całemu personelowi, którego dotyczą, oraz zintegrowane ze zaktualizowanymi procedurami i programami podnoszenia świadomości

9.4 Walidacja po przeglądzie musi potwierdzić, że zaktualizowane wymagania zostały odzwierciedlone w Rejestrze audytów, narzędziach zgodności i wewnętrznych pulpitach monitorowania.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest spójna z następującymi powiązanymi politykami organizacyjnymi:

10.1.1 P1 – Polityka bezpieczeństwa informacji: określa SZBI i ustanawia rozliczalność za zgodność oraz ciągłe doskonalenie

10.1.2 P5 – Polityka zarządzania zmianą: zapewnia widoczność audytową zmian infrastruktury i konfiguracji wpływających na środowiska kontrolne

10.1.3 P6 – Polityka zarządzania ryzykiem: integruje wyniki audytów z działaniami organizacji w zakresie oceny ryzyka i postępowania z ryzykiem

10.1.4 P14 – Polityka retencji i utylizacji danych: reguluje okres przechowywania dowodów audytowych, logów i zapisów zgodności

10.1.5 P18 – Polityka zabezpieczeń kryptograficznych: wspiera bezpieczne przechowywanie i przekazywanie wrażliwych danych audytowych

10.1.6 P26 – Polityka bezpieczeństwa dostawców i stron trzecich: obejmuje prawa do audytu, dokumentację zapewnienia oraz nadzór nad zgodnością dostawców

10.1.7 P30 – Polityka reagowania na incydenty: zapewnia spójność audytów procesów obsługi incydentów z celami zapewnienia SZBI

10.1.8 P32 – Polityka ciągłości działania i odtwarzania po awarii: wymaga weryfikacji testów ciągłości działania i zgodności z DRP w ramach cykli audytowych

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z globalnymi normami i wymaganiami prawnymi w zakresie audytu oraz ciągłej walidacji zgodności.

11.2 ISO/IEC 27001:

11.2.1 Klauzula 9.2 – audyt wewnętrzny: wymaga regularnych, opartych na ryzyku audytów SZBI w celu oceny skuteczności i zgodności.

11.2.2 Klauzula 9.3 – przegląd zarządzania: wyniki audytów muszą stanowić dane wejściowe do przeglądu strategicznego i działań doskonalących.

11.2.3 Klauzula 10.1 – niezgodność i działanie korygujące: ustalenia audytowe muszą być obsługiwane za pomocą udokumentowanych procedur CAPA.

11.3 ISO/IEC 27002:2022 – zabezpieczenia 5.35–5.37:

11.3.1 Zabezpieczenia z Załącznika A 5.35–5.37: obejmują niezależny przegląd, zgodność z wymaganiami prawnymi i umownymi oraz rejestrowanie audytowe.

11.3.2 Zapewniają wytyczne wdrożeniowe dotyczące planowania, realizacji i doskonalenia programów audytu oraz zgodności.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – oceny zabezpieczeń: wymaga rutynowego przeglądu wdrożonych zabezpieczeń bezpieczeństwa.

11.4.2 CA-5 – Plan działań i kamienie milowe (POA&M): wspiera śledzenie i remediację ustaleń audytowych.

11.4.3 CA-7 – ciągłe monitorowanie: wspiera proaktywne, zautomatyzowane oceny zgodności.

11.5 RODO (2016/679):

11.5.1 Artykuły 24 i 32: wymagają dowodów wdrożenia i skuteczności zabezpieczeń bezpieczeństwa poprzez odpowiednie struktury ładu organizacyjnego.

11.5.2 Artykuł 33: potwierdza potrzebę utrzymywania zweryfikowanych ścieżek audytowych na potrzeby reagowania na naruszenia i realizacji obowiązków notyfikacyjnych.

11.6 Dyrektywa NIS2 (2022/2555):

11.6.1 Artykuł 21(2)(g): wymaga audytowania polityk i procedur jako elementu minimalnych środków zarządzania ryzykiem w cyberbezpieczeństwie.

11.6.2 Artykuł 27: organy krajowe mogą prowadzić audyty lub wymagać ich przeprowadzenia wobec podmiotów kluczowych i ważnych.

11.7 Rozporządzenie DORA (2022/2554):

11.7.1 Artykuł 10(2)(e): podmioty muszą prowadzić audyty wewnętrzne i zewnętrzne praktyk zarządzania ryzykiem ICT.

11.7.2 Artykuł 25 – wymagania audytowe: nakłada obowiązek okresowych audytów prowadzonych przez audytorów wewnętrznych lub niezależnych audytorów zewnętrznych, przy zapewnieniu widoczności regulacyjnej.

11.8 COBIT 2019:

11.8.1 MEA01 – monitorowanie, ocena i analiza wydajności oraz zgodności: zapewnia weryfikację skuteczności zabezpieczeń i raportowanie jej do organów ładu organizacyjnego.

11.8.2 MEA03 – monitorowanie, ocena i analiza zgodności: wymaga dostosowania praktyk organizacji do wymagań prawnych, umownych i opartych na normach.