					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P33S					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, 10	Audyty wewnętrzne, ciągłe doskonalenie oraz usuwanie niezgodności
ISO/IEC 27002:2022	Środki kontrolne 5.35, 5.37	Planowane przeglądy wewnętrzne, niezależne przeglądy procesów realizowanych w outsourcingu
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Oceny bezpieczeństwa, ciągłe monitorowanie zgodności, przegląd, analiza i raportowanie audytowe
RODO	Artykuły 24 i 32	Audyt środków technicznych i organizacyjnych oraz dowody skuteczności zabezpieczeń
Dyrektywa NIS2	Artykuł 21(2)(f)	Proaktywny przegląd oraz zgodność oparta na dowodach
Rozporządzenie DORA	Artykuł 10	Zarządzanie ryzykiem ICT, monitorowanie i raportowanie
COBIT 2019	MEA01, MEA03	Monitorowanie i ocena zgodności oraz gotowość do przeglądów prowadzonych przez strony trzecie

1. Cel

1.1 Niniejsza polityka określa podejście organizacji do prowadzenia audytów wewnętrznych, weryfikacji środków kontroli bezpieczeństwa oraz monitorowania zgodności z wymaganiami regulacyjnymi. Zapewnia, że wszystkie środki kontrolne, polityki, systemy i dostawcy usług podlegają regularnemu i ustrukturyzowanemu przeglądowi.

1.2 Celem polityki jest wykrywanie nieskuteczności środków kontroli, zapobieganie niezgodnościom oraz wykazywanie należytej staranności zgodnie z ISO/IEC 27001, RODO i powiązanymi ramami odniesienia.

1.3 Polityka umożliwia MŚP utrzymanie kontroli operacyjnej i gotowości do certyfikacji, nawet bez wydzielonej funkcji zgodności, poprzez stosowanie prostych, powtarzalnych list kontrolnych oraz ustaleń priorytetyzowanych według ryzyka.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich działów wewnętrznych oraz zewnętrznych dostawców usług realizujących obowiązki związane z systemami IT, danymi osobowymi i systemami krytycznymi dla biznesu,

2.1.2 wszystkich środków kontroli i systemów objętych zakresem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),

2.1.3 wszystkich audytów wewnętrznych, przeglądów środków kontroli bezpieczeństwa i kontroli zgodności — niezależnie od tego, czy są realizowane wewnętrznie, czy przez konsultanta zewnętrznego, klienta lub organ regulacyjny.

2.2 Niniejsza polityka ma również zastosowanie do gromadzenia dowodów i raportowania na potrzeby:

2.2.1 audytów certyfikacyjnych i recertyfikacyjnych ISO/IEC 27001,

2.2.2 audytów ochrony danych prowadzonych na podstawie RODO lub wymagań umownych,

2.2.3 kwestionariuszy bezpieczeństwa inicjowanych przez klientów lub przeglądów due diligence,

2.2.4 wszelkich przeglądów regulacyjnych lub niezależnych prowadzonych na podstawie NIS2 lub DORA, jeżeli mają zastosowanie.

3. Cele

3.1 Zapewnienie, że wszystkie kluczowe środki kontrolne i polityki są regularnie poddawane przeglądowi pod kątem skuteczności i zgodności.

3.2 Utrzymywanie ścieżek audytowych oraz zapisów działań korygujących w celu wykazania rozliczalności i doskonalenia.

3.3 Przygotowanie do certyfikacji, recertyfikacji i programów zapewnienia dla klientów (np. ISO 27001, onboarding dostawcy).

3.4 Wczesna identyfikacja luk w celu umożliwienia szybkiego podjęcia działań naprawczych, zanim problemy eskalują lub doprowadzą do naruszenia obowiązków.

3.5 Umożliwienie Dyrektorowi Generalnemu i dostawcy wsparcia IT koordynacji przeglądów przy minimalnej złożoności, z zachowaniem wyników możliwych do obrony podczas audytu lub kontroli.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 sprawuje nadzór nad programem audytów,

4.1.2 zatwierdza plany przeglądów wewnętrznych i ustalenia,

4.1.3 przypisuje działania korygujące i monitoruje ich realizację,

4.1.4 upoważnia do zaangażowania zewnętrznych audytorów lub konsultantów.

4.2 Dostawca usług IT / Administrator

4.2.1 dostarcza dowody podczas audytów wewnętrznych i zewnętrznych (np. logi, konfiguracje, zapisy kontroli dostępu),

4.2.2 wspiera weryfikację techniczną (np. status kopii zapasowych, zgodność w zakresie poprawek),

4.2.3 utrzymuje repozytorium dowodów audytowych.

[... 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 polityki i planu audytów

9.1.1 Dyrektor Generalny (GM) musi dokonać przeglądu niniejszej polityki i harmonogramu audytów co najmniej raz w roku.

9.1.2 Przegląd musi obejmować ocenę:

9.1.2.1 skuteczności audytów w identyfikowaniu luk,

9.1.2.2 wskaźnika realizacji audytów i działań korygujących,

9.1.2.3 zmian w mających zastosowanie wymaganiach prawnych, regulacyjnych lub certyfikacyjnych.

9.2 Aktualizacje inicjowane zdarzeniami

9.2.1 Polityka musi zostać poddana przeglądowi i zaktualizowana, gdy:

9.2.2 audyt certyfikacyjny lub audyt nadzoru zakończy się istotną niezgodnością,

9.2.3 zmianie ulegną ramy prawne lub regulacyjne (np. nowe wytyczne dotyczące RODO, krajowe wdrożenie NIS2),

9.2.4 zmiany biznesowe wpłyną na systemy, procesy lub dostawców objętych zakresem audytu,

9.2.5 krytyczny incydent lub naruszenie ujawni wcześniej niewykryte luki w środkach kontroli.

9.3 Dokumentowanie aktualizacji

9.3.1 Wszystkie zmiany muszą być odnotowywane w rejestrze historii wersji polityki.

9.3.2 Aktualizacje muszą zostać przekazane wszystkim członkom zespołu zaangażowanym w audyty.

9.3.3 Do zaktualizowanej polityki należy dołączyć podsumowanie zmian w celu zapewnienia ich zrozumienia.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest wspierana przez kilka innych polityk MŚP i wzmacnia ich stosowanie:

10.1.1 P1S – Polityka bezpieczeństwa informacji: określa bazowy poziom oczekiwań wobec środków kontroli i wymaga ich weryfikacji w drodze audytów.

10.1.2 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: ustanawia rozliczalność za planowanie audytów, ich realizację oraz odpowiedzialność za działania korygujące.

10.1.3 P6S – Polityka zarządzania ryzykiem: identyfikuje słabości środków kontroli ujawnione w audytach i zapewnia dokumentowanie ustaleń w rejestrze ryzyk.

10.1.4 P17S – Polityka ochrony danych i prywatności: określa środki kontroli RODO podlegające audytowi, w tym przetwarzanie danych, reagowanie na naruszenia i klauzule informacyjne.

10.1.5 P22S – Polityka rejestrowania zdarzeń i monitorowania: dostarcza logi audytowe i dane kryminalistyczne wykorzystywane podczas przeglądów zgodności i kontroli.

10.1.6 P30S – Polityka reagowania na incydenty: wymaga okresowego audytu zapisów incydentów i przeglądów po incydencie w celu weryfikacji skuteczności reakcji.

10.1.7 P31S – Polityka gromadzenia dowodów i kryminalistyki: określa procedury pozyskiwania weryfikowalnych dowodów z zachowaniem łańcucha nadzoru podczas audytów.

10.2 Łącznie polityki te tworzą zamknięte środowisko kontrolne, które umożliwia weryfikację wewnętrzną, zewnętrzne zapewnienie oraz ład zarządczy zgodny z normami.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001:

11.1.1 Klauzula 9.2 – wymaga prowadzenia audytów wewnętrznych w celu oceny skuteczności SZBI oraz zgodności z wymaganiami.

11.1.2 Klauzula 10.1 – wymaga ciągłego doskonalenia na podstawie wyników audytów oraz usuwania niezgodności.

11.2 ISO/IEC 27002:

11.2.1 Środek kontrolny 5.35 – wymaga planowanych przeglądów wewnętrznych środków kontroli i procesów.

11.2.2 Środek kontrolny 5.37 – podkreśla znaczenie niezależnych przeglądów, zwłaszcza dla procesów realizowanych w outsourcingu.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Oceny bezpieczeństwa: wymaga audytowania wdrożonych środków kontroli w celu potwierdzenia ich skuteczności.

11.3.2 CA-7 – Ciągłe monitorowanie zgodności: podkreśla proaktywne wykrywanie słabości środków kontroli i ich przegląd.

11.3.3 AU-6 – Przegląd, analiza i raportowanie audytowe: wymaga regularnej analizy logów audytowych i ustaleń oraz ich rozliczenia.

11.4 RODO:

11.4.1 Artykuły 24 i 32 – wymagają wdrożenia i audytowania środków technicznych i organizacyjnych, w tym dowodów skuteczności środków kontroli i doskonalenia w czasie.

11.5 Dyrektywa UE NIS2 (2022/2555):

11.5.1 Artykuły 20–21 – wymagają proaktywnego przeglądu środków kontroli, zgodności opartej na dowodach oraz zapewnienia prześledzalności audytowej dla podmiotów kluczowych i ważnych.

11.6 COBIT 2019:

11.6.1 MEA01 – Monitorowanie, ocena i ocena wydajności oraz zgodności: wymaga okresowej oceny wydajności procesów i środków kontroli względem norm i celów.

11.6.2 MEA03 – Zapewnienie zgodności z wymaganiami zewnętrznymi: koncentruje się na monitorowaniu wewnętrznym oraz gotowości do audytów stron trzecich i przeglądów regulacyjnych.