					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P08S					Tytuł dokumentu: **Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji**							
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 odpowiednich norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 7	
ISO/IEC 27002:2022	Środek kontrolny 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
Dyrektywa NIS2	Artykuł 21 ust. 2 lit. i	
Rozporządzenie DORA	Artykuł 13	
COBIT 2019	BAI08, DSS	
RODO	Artykuł 32, 39	

1. Cel

1.1. Niniejsza polityka zapewnia, że wszyscy pracownicy i współpracownicy rozumieją swoje obowiązki w zakresie bezpieczeństwa informacji.

1.2. Jej celem jest ograniczenie prawdopodobieństwa błędu ludzkiego, zwiększenie zdolności wykrywania i zgłaszania incydentów oraz wzmacnianie kultury bezpieczeństwa w całej organizacji.

1.3. Polityka wspiera zgodność z ISO/IEC 27001, NIS2, RODO i DORA poprzez włączenie świadomości bezpieczeństwa do codziennych zachowań w pracy oraz oczekiwań związanych z pełnioną rolą.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich pracowników, współpracowników, stażystów oraz stron trzecich, które mają dostęp do systemów lub danych organizacji.

2.2. Obejmuje ona:

2.2.1. Szkolenie wstępne z zakresu świadomości bezpieczeństwa dla nowo zatrudnionego personelu

2.2.2. Coroczne szkolenie przypominające z zakresu bezpieczeństwa

2.2.3. Szkolenia doraźne i działania podnoszące świadomość (np. komunikaty związane z incydentami, plakaty lub wskazówki)

2.3. Polityka obowiązuje we wszystkich rolach, działach i lokalizacjach pracy.

3. Cele

3.1. Zapewnić, aby cały personel otrzymywał terminowe, zrozumiałe i adekwatne szkolenia uświadamiające w zakresie bezpieczeństwa informacji.

3.2. Zapewnić pracownikom zdolność identyfikowania i unikania powszechnych zagrożeń, takich jak phishing, złośliwe oprogramowanie i wycieki danych.

3.3. Zapewnić dokumentowanie ukończenia szkoleń w celu wykazania zgodności z wymaganiami prawnymi, umownymi i audytowymi.

3.4. Utrzymywać aktualne treści szkoleniowe, odzwierciedlające polityki organizacji, zagrożenia i mające zastosowanie regulacje.

3.5. Wzmacniać wśród personelu proaktywne podejście, w ramach którego bezpieczeństwo jest traktowane jako element codziennej odpowiedzialności.

4. Role i odpowiedzialności

4.1. Dyrektor Generalny

4.1.1. Zatwierdza wymagania szkoleniowe i zapewnia przydzielenie odpowiednich zasobów.

4.1.2. Przegląda raporty dotyczące ukończenia szkoleń i w razie potrzeby eskaluje przypadki braku zgodności.

4.2. Office Manager / Dział HR

4.2.1. Koordynuje realizację szkoleń dla nowo zatrudnionych oraz corocznych szkoleń przypominających.

4.2.2. Utrzymuje rejestry szkoleń i dzienniki ukończenia szkoleń.

4.2.3. Zapewnia uzyskanie od personelu potwierdzenia zapoznania się z kluczowymi politykami bezpieczeństwa oraz z umową o zachowaniu poufności.

[... 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 podlegać corocznemu przeglądowi przez Dyrektora Generalnego oraz HR w celu zapewnienia, że odzwierciedla aktualne ryzyka, regulacje i potrzeby personelu.

9.2. Aktualizacje międzyokresowe

9.2.1. Treść polityki i materiałów szkoleniowych musi również podlegać przeglądowi i aktualizacji po:

9.2.1.1. Poważnym incydencie bezpieczeństwa

9.2.1.2. Zmianach prawnych lub umownych

9.2.1.3. Restrukturyzacji organizacyjnej lub migracjach systemów

9.3. Kontrola wersji i dystrybucja

9.3.1. Każda aktualizacja musi obejmować:

9.3.1.1. Numer wersji i datę wejścia w życie

9.3.1.2. Podsumowanie zmian

9.3.1.3. Zatwierdzenie przez Dyrektora Generalnego

9.3.1.4. Archiwum wszystkich wcześniejszych wersji przechowywane przez co najmniej trzy lata

9.4. Komunikacja do pracowników

9.4.1. Aktualizacje polityki muszą zostać zakomunikowane całemu personelowi, a w przypadku zmian istotnych należy uzyskać potwierdzenie zapoznania się.

10. Polityki powiązane i zależności

10.1. Niniejsza polityka wspiera następujące dokumenty:

10.1.1. P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: przypisuje odpowiedzialność za koordynację szkoleń i nadzór

10.1.2. P3S – Polityka dopuszczalnego użytkowania: wzmacnia oczekiwania dotyczące zachowań omawianych podczas szkoleń

10.1.3. P4S – Polityka kontroli dostępu: zapewnia, że użytkownicy rozumieją znaczenie bezpieczeństwa dostępu

10.1.4. P7S – Polityka wdrażania i zakończenia współpracy: włącza szkolenia do procesu wdrożenia

10.1.5. P30S – Polityka reagowania na incydenty: zapewnia, że personel wie, jak zgłaszać incydenty terminowo i prawidłowo

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 7.3 – wymaga, aby organizacje zapewniały świadomość personelu w zakresie jego obowiązków i wpływu na bezpieczeństwo

11.2. ISO/IEC 27002

11.2.1. Środek kontrolny 6.3 – określa wymagania dotyczące zakresu i sposobu realizacji szkoleń z zakresu bezpieczeństwa

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – wymaga szkoleń uświadamiających dla użytkowników mających dostęp do systemów

11.3.2. AT-4 – obejmuje szkolenia oparte na rolach oraz konsekwencje braku zgodności

11.4. RODO

11.4.1. Artykuł 32 – wymaga stosowania środków bezpieczeństwa, w tym szkoleń personelu, w celu ochrony danych osobowych

11.4.2. Artykuł 39 – wymaga, aby inspektor ochrony danych nadzorował działania w zakresie świadomości i szkoleń, w stosownych przypadkach

11.5. Dyrektywa NIS2

11.5.1. Artykuł 21 ust. 2 lit. i – wymaga prowadzenia ciągłych programów w zakresie świadomości cyberbezpieczeństwa i szkoleń

11.6. Rozporządzenie DORA

11.6.1. Artykuł 13 – wymaga, aby podmioty finansowe wdrożyły działania edukacyjne i szkoleniowe dla całego personelu posiadającego obowiązki związane z ICT

11.7. COBIT 2019

11.7.1. BAI08 – Zarządzanie wiedzą: zapewnia, że personel posiada odpowiednie kompetencje i przeszkolenie

11.7.2. DSS05 – Zarządzanie usługami bezpieczeństwa: podkreśla znaczenie świadomości jako kluczowej kontroli zapobiegawczej