					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P08					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 7.3, Załącznik A, zabezpieczenie 6.3	Określa wymagania dotyczące świadomości i szkoleń objętych niniejszą polityką
ISO/IEC 27002:2022	Zabezpieczenie 6	Wspiera odpowiednie szkolenia uświadamiające dostosowane do roli zawodowej
NIST SP 800-53 Rev.5	AT-1 do AT-5	Jest zgodny z wymaganiami dotyczącymi polityk i procedur, szkoleń uświadamiających, szkoleń specyficznych dla roli, zapisów szkoleń oraz kontaktu z grupą bezpieczeństwa
RODO	Artykuły 32, 39; motyw 78	Nakłada obowiązek szkolenia osób przetwarzających dane osobowe oraz budowania ogólnej świadomości personelu
Dyrektywa NIS2	Artykuły 21(2)(a, b), 21(3)	Wymaga polityk dotyczących szkoleń w zakresie ryzyka i bezpieczeństwa oraz inicjatyw budowania świadomości
Rozporządzenie DORA	Artykuły 5, 8, 13	Wymaga uwzględnienia świadomości ryzyka ICT i szkoleń jako elementu zabezpieczeń odporności operacyjnej
COBIT 2019	Zarządzanie zasobami ludzkimi, DSS05 Zarządzanie usługami bezpieczeństwa, MEA	Wzmacnia wymagania dotyczące świadomości pracowników, edukacji użytkowników oraz monitorowania zgodności

1. Cel

1.1 Niniejsza polityka ustanawia formalne ramy zapewniające, że cały personel jest świadomy swoich obowiązków w zakresie bezpieczeństwa informacji oraz otrzymuje szkolenia niezbędne do ochrony poufności, integralności i dostępności (CIA) aktywów informacyjnych.

1.2 Wspiera wymagania ISO/IEC 27001, klauzuli 7.3 oraz Załącznika A, zabezpieczenia 6.3, poprzez ustanowienie uporządkowanego programu świadomości i szkoleń opartego na ryzyku, dostosowanego do ról organizacyjnych i zmieniających się zagrożeń.

1.3 Polityka przyczynia się do ograniczenia podatności związanych z czynnikiem ludzkim, promowania zachowań świadomych bezpieczeństwa oraz ciągłego wzmacniania bezpiecznych praktyk zgodnie z wymogami regulacyjnymi i umownymi.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich osób wewnętrznych i zewnętrznych posiadających dostęp do systemów informatycznych organizacji, danych lub obiektów, w tym:

2.1.1 pracowników (pełnoetatowych, niepełnoetatowych, tymczasowych)

2.1.2 wykonawców, konsultantów, dostawców i stażystów

2.1.3 stron trzecich posiadających dostęp logiczny lub fizyczny na podstawie umów o świadczenie usług

2.2 Zakres obejmuje:

2.2.1 wstępne szkolenie w zakresie świadomości bezpieczeństwa

2.2.2 szkolenie specyficzne dla roli (np. programiści, finanse, użytkownicy uprzywilejowani)

2.2.3 okresowe szkolenia przypominające i kampanie budowania świadomości

2.2.4 szkolenia doraźne w odpowiedzi na incydenty lub nowe zagrożenia

2.3 Metody realizacji szkoleń objęte niniejszą polityką obejmują e-learning, szkolenia stacjonarne, symulacje, testy wiedzy, plakaty, biuletyny bezpieczeństwa oraz obowiązkowe potwierdzenia zapoznania się.

3. Cele

3.1 Zapewnienie, że cały personel rozumie swoje obowiązki w zakresie ochrony aktywów organizacji i przestrzegania polityk bezpieczeństwa.

3.2 Zapewnienie ciągłych, mierzalnych szkoleń uświadamiających dostosowanych do ekspozycji na ryzyko wynikającej z roli.

3.3 Utrwalenie bezpiecznych zachowań w codziennych działaniach operacyjnych poprzez wzmacnianie takich praktyk jak bezpieczne korzystanie z haseł, zgłaszanie incydentów oraz odporność na phishing.

3.4 Zapewnienie zgodności regulacyjnej oraz gotowości audytowej w zakresie wymogów szkoleniowych dotyczących bezpieczeństwa informacji w różnych branżach i jurysdykcjach.

3.5 Ograniczenie incydentów bezpieczeństwa wynikających z niedbalstwa, braku świadomości lub błędnej oceny sytuacji poprzez kształtowanie zachowań i ciągłe utrwalanie właściwych praktyk.

4. Role i obowiązki

4.1 Kierownictwo wykonawcze

4.1.1 Zatwierdza strategię szkoleń w zakresie bezpieczeństwa informacji organizacji oraz zapewnia zasoby i uwzględnienie jej w priorytetach organizacji.

4.1.2 Monitoruje zgodność na poziomie zarządczym oraz zapewnia przestrzeganie polityki we wszystkich działach.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO) / Menedżer systemu zarządzania bezpieczeństwem informacji

4.2.1 Odpowiada za niniejszą politykę oraz definiuje ramy podnoszenia świadomości i szkoleń zgodnie z ryzykiem, wymaganiami zgodności i potrzebami biznesowymi.

4.2.2 Nadzoruje projektowanie, realizację, monitorowanie i przegląd wszystkich inicjatyw szkoleniowych z zakresu bezpieczeństwa.

4.2.3 Zapewnia, że szkolenia są okresowo aktualizowane i odzwierciedlają ewoluujące zagrożenia oraz nowe technologie.

[... 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 Częstotliwość przeglądu

9.1.1 Niniejsza polityka oraz powiązany program szkoleniowy muszą być poddawane przeglądowi:

9.1.1.1 corocznie, lub

9.1.1.2 po poważnych incydentach związanych z błędem ludzkim lub zagrożeniem wewnętrznym

9.1.1.3 przy wprowadzaniu istotnych nowych technologii lub zagrożeń

9.1.1.4 w odpowiedzi na zmiany obowiązków prawnych, umownych lub certyfikacyjnych

9.2 Proces przeglądu

9.2.1 Przegląd prowadzi CISO w uzgodnieniu z:

9.2.1.1 działami HR i szkoleń

9.2.1.2 osobami odpowiedzialnymi za obszar prawny i ochronę danych

9.2.1.3 funkcjami bezpieczeństwa IT i ryzyka operacyjnego

9.2.2 Wszystkie aktualizacje muszą być:

9.2.2.1 zatwierdzone przez Komitet Sterujący ds. Bezpieczeństwa Informacji

9.2.2.2 objęte kontrolą wersji i udokumentowane w rejestrze dokumentów SZBI

9.2.2.3 komunikowane użytkownikom, jeżeli istotne zmiany wpływają na zakres szkolenia lub obowiązki

9.3 Nadzór nad aktualizacją treści

9.3.1 Moduły szkoleniowe i materiały uświadamiające muszą być przeglądane co 12 miesięcy w celu zapewnienia:

9.3.1.1 adekwatności do krajobrazu zagrożeń

9.3.1.2 poprawności regulacyjnej

9.3.1.3 zgodności formatu (np. dostępność, lokalizacja)

9.3.2 Nieaktualne lub wprowadzające w błąd treści muszą być niezwłocznie wycofywane i zastępowane zatwierdzonymi alternatywami.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest wspierana przez następujące dokumenty i wspiera stosowanie ich postanowień:

10.1.1 P01 – Polityka bezpieczeństwa informacji: Ustanawia świadomość bezpieczeństwa jako bazowe zabezpieczenie w SZBI organizacji.

10.1.2 P03 – Polityka dopuszczalnego użytkowania: Wymaga potwierdzenia przez użytkownika w trakcie szkolenia i precyzuje obowiązki związane z codziennym korzystaniem z technologii.

10.1.3 P07 – Polityka wdrażania i zakończenia współpracy: Zapewnia uwzględnienie szkoleń na etapie wdrożenia oraz ich śledzenie przez cały okres zatrudnienia.

10.1.4 P06 – Polityka zarządzania ryzykiem: Łączy szkolenia ukierunkowane na czynnik ludzki z modelowaniem zagrożeń i strategiami ograniczania ryzyka rezydualnego.

10.1.5 P33 – Polityka audytu i monitorowania zgodności: Potwierdza, że zabezpieczenia związane ze świadomością są operacyjne, mierzalne i skuteczne podczas audytów.

10.2 Łącznie polityki te tworzą kompleksowe ramy zabezpieczeń behawioralnych, które integrują świadomość, rozliczalność i wzmacnianie kultury organizacyjnej.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 7.3 – Świadomość: Wymaga, aby organizacje zapewniały, że pracownicy są świadomi polityk bezpieczeństwa informacji i swoich obowiązków. Niniejsza polityka realizuje ten wymóg poprzez uporządkowane wdrożenie, szkolenia okresowe i mierzalny udział w kampaniach.

11.1.2 Załącznik A, zabezpieczenie 6.3 – Świadomość, edukacja i szkolenia w zakresie bezpieczeństwa informacji: W pełni realizowane poprzez wstępne, oparte na rolach i ciągłe programy szkoleniowe dostosowane do profili ryzyka użytkowników.

11.2 ISO/IEC 27002:2022 – Zabezpieczenie 6

11.2.1 Wspiera opracowanie i realizację szkoleń uświadamiających odpowiednich do ról zawodowych, z naciskiem na wzmacnianie bezpiecznych zachowań oraz okresowe aktualizacje oparte na informacjach o zagrożeniach i wnioskach z audytów.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 do AT-5 (rodzina Awareness and Training): Niniejsza polityka jest zgodna z AT-1 (Polityka i procedury), AT-2 (Szkolenie uświadamiające), AT-3 (szkolenie specyficzne dla roli), AT-4 (zapisy szkoleń z zakresu bezpieczeństwa) oraz AT-5 (kontakt z grupami bezpieczeństwa).

11.3.2 IA-5, AC-2: Wzmacnia odpowiedzialność użytkownika za bezpieczne uwierzytelnianie i dopuszczalne użytkowanie aktywów organizacji — kluczowe elementy behawioralnych efektów programów budowania świadomości.

11.3.3 IR-1 do IR-8: Gotowość reagowania na incydenty jest wzmacniana poprzez ukierunkowane kampanie budowania świadomości i symulacje.

11.4 RODO (2016/679)

11.4.1 Artykuł 32 – Bezpieczeństwo przetwarzania: Wymaga, aby personel przetwarzający dane osobowe był szkolony w rozpoznawaniu, zapobieganiu i zgłaszaniu ryzyk dotyczących danych osobowych. Niniejsza polityka zapewnia odpowiednie szkolenie osób przetwarzających dane oraz wszystkich właściwych ról.

11.4.2 Artykuł 39 – Zadania inspektora ochrony danych: Obejmują podnoszenie świadomości i szkolenie personelu uczestniczącego w operacjach przetwarzania.

11.4.3 Motyw 78: Zachęca do stosowania odpowiednich działań uświadamiających w celu zapewnienia solidnych praktyk bezpieczeństwa i przestrzegania polityk.

11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(a, b): Wymaga, aby podmioty przyjmowały polityki dotyczące analizy ryzyka i szkoleń z zakresu bezpieczeństwa dla całego właściwego personelu. Niniejsza polityka spełnia ten wymóg poprzez ustanowienie ciągłych procesów szkoleniowych dostosowanych do ról.

11.5.2 Artykuł 21(3): Zachęca do promowania świadomości ryzyka cyberbezpieczeństwa wśród kadry zarządzającej i personelu poprzez inicjatywy uświadamiające i symulacje.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 13 – Strategia cyfrowej odporności operacyjnej: Wymaga, aby świadomość ryzyka ICT i szkolenia stanowiły część modelu ładu zarządczego. Niniejsza polityka zapewnia uwzględnienie ryzyka związanego z czynnikiem ludzkim poprzez ciągłą edukację i symulacje zagrożeń.

11.6.2 Artykuły 5 i 8: Podkreślają znaczenie ram kontroli wewnętrznej, których świadomość i szkolenia są podstawowymi elementami odporności ICT i cyberhigieny.

11.7 COBIT 2019

11.7.1 Zarządzanie zasobami ludzkimi – Managed Human Resources: Wzmacnia potrzebę rozwijania świadomości obowiązków w zakresie bezpieczeństwa i osadzania jej w zarządzaniu personelem.

11.7.2 DSS05 Zarządzanie usługami bezpieczeństwa – Managed Security Services: Ustanawia zabezpieczenia dotyczące edukacji użytkowników i zgłaszania incydentów, które stanowią integralną część niniejszej polityki.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Wymaga przeglądu skuteczności zachowań użytkowników i przestrzegania polityk — realizowanego tutaj poprzez testy phishingowe, testy wiedzy i wskaźniki kampanii budowania świadomości.