					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P13					Tytuł dokumentu: **Polityka klasyfikacji i oznaczania 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**

1. Cel

1.1 Niniejsza polityka ustanawia formalne ramy klasyfikacji i oznaczania aktywów informacyjnych organizacji na podstawie ich wrażliwości, ekspozycji na ryzyko oraz obowiązków regulacyjnych.

1.2 Zapewnia ona, że wszystkie informacje — niezależnie od tego, czy są przechowywane, przesyłane czy przetwarzane — są jednoznacznie klasyfikowane i oznaczane w sposób wskazujący wymagany poziom ochrony oraz zasady postępowania.

1.3 Polityka wymaga stosowania ustrukturyzowanej klasyfikacji zgodnej z praktykami organizacji w zakresie zarządzania ryzykiem, wspierając cele w obszarze poufności, integralności i dostępności (CIA) zarówno dla danych cyfrowych, jak i fizycznych.

1.4 Ten środek kontrolny jest niezbędny do umożliwienia kontroli dostępu opartej na rolach, zapewnienia gotowości audytowej, właściwego udostępniania danych oraz skutecznego wdrożenia zabezpieczeń technicznych, takich jak szyfrowanie, systemy kopii zapasowych i monitorowanie.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich aktywów informacyjnych organizacji, w tym dokumentów, baz danych, zapisów i komunikacji,

2.1.2 wszystkich formatów danych, w tym cyfrowych, drukowanych, pisemnych i ustnych,

2.1.3 wszystkich środowisk, w tym infrastruktury lokalnej, środowisk zdalnych, mobilnych oraz chmury obliczeniowej,

2.1.4 wszystkich pracowników, kontrahentów, dostawców usług oraz podmiotów trzecich przetwarzających dane, którzy tworzą, przetwarzają lub przechowują informacje organizacji.

2.2 Zakres obejmuje treści tworzone wewnętrznie, dane pozyskiwane z zewnątrz, dane osobowe objęte obowiązkami wynikającymi z przepisów o ochronie prywatności (np. RODO) oraz informacje wymieniane z klientami, partnerami i organami regulacyjnymi.

2.3 Polityka ma zastosowanie do wszystkich systemów wykorzystywanych do przechowywania lub przesyłania danych, w tym aplikacji korporacyjnych, serwerów plików, systemów poczty elektronicznej, platform chmurowych oraz repozytoriów kopii zapasowych.

3. Cele

3.1 Ustanowienie ustandaryzowanego, obowiązującego w całej organizacji schematu klasyfikacji opartego na wpływie ujawnienia lub naruszenia danych.

3.2 Zapewnienie, że wszystkie informacje są oznaczane w sposób widoczny i trwały, tak aby odzwierciedlały poziom klasyfikacji oraz wymagania dotyczące postępowania.

3.3 Egzekwowanie zasad postępowania z danymi i kontroli dostępu zgodnych z klasyfikacją, w tym szyfrowania, rejestrowania, ochrony transmisji oraz okresów przechowywania.

3.4 Wspieranie zgodności z międzynarodowymi normami (ISO/IEC 27001, 27002), ramami prawnymi (RODO, NIS2, DORA) oraz wewnętrznymi politykami zarządzania ryzykiem.

3.5 Zapewnienie, że wszyscy użytkownicy rozumieją swoje obowiązki w zakresie ochrony danych, stosowania oznaczeń oraz prawidłowego postępowania z informacjami sklasyfikowanymi.

3.6 Utrzymanie identyfikowalności pomiędzy statusem klasyfikacji, powiązanymi środkami kontrolnymi oraz inwentarzem aktywów organizacji na potrzeby audytu i zgodności.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO)

4.1.1 Odpowiada za politykę klasyfikacji i oznaczania informacji oraz zapewnia jej zgodność z wymaganiami regulacyjnymi, umownymi i operacyjnymi.

4.1.2 Zatwierdza poziomy klasyfikacji, standardy oznaczania oraz zmiany polityki.

4.1.3 Nadzoruje zgodność z polityką poprzez audyty, wskaźniki oraz przeglądy odstępstw.

4.1.4 Koordynuje nadzór międzyfunkcyjny z zespołami ds. prawnych i zgodności, ochrony danych oraz zarządzania ryzykiem.

4.2 Właściciele informacji

4.2.1 Odpowiadają za klasyfikację aktywów informacyjnych pozostających pod ich nadzorem zgodnie ze schematem klasyfikacji obowiązującym w organizacji.

4.2.2 Stosują oznaczenia klasyfikacyjne w momencie utworzenia, aktualizacji lub przyjęcia informacji.

4.2.3 Okresowo dokonują przeglądu klasyfikacji aktywów, w szczególności w odpowiedzi na zmiany wrażliwości, zakresu regulacyjnego lub wartości biznesowej.

4.2.4 Zapewniają właściwe postępowanie z danymi wrażliwymi i ich oznaczanie w całym cyklu życia.

[... 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 podlegać przeglądowi co najmniej raz w roku w celu zapewnienia zgodności z:

9.1.1 zmieniającymi się wymaganiami regulacyjnymi (np. RODO, NIS2, DORA),

9.1.2 aktualizacjami wytycznych ISO/IEC 27001 lub 27002 dotyczących klasyfikacji,

9.1.3 zmianami organizacyjnymi wpływającymi na wrażliwość danych lub ich właściciela,

9.1.4 zmianami technologicznymi, w tym nowymi platformami zarządzania dokumentami lub danymi.

9.2 Dyrektor ds. Bezpieczeństwa Informacji (CISO) inicjuje przegląd we współpracy z Komitetem ds. Bezpieczeństwa Informacji, działem prawnym oraz właściwymi jednostkami biznesowymi.

9.3 Przeglądy muszą obejmować:

9.3.1 skuteczność egzekwowania klasyfikacji i przestrzegania zasad przez użytkowników,

9.3.2 analizę incydentów lub odstępstw związanych z błędną klasyfikacją,

9.3.3 informacje zwrotne od użytkowników dotyczące narzędzi oznaczania lub materiałów instruktażowych,

9.3.4 porównanie z branżowymi standardami klasyfikacji.

9.4 Aktualizacje polityki muszą podlegać kontroli wersji, być dokumentowane w repozytorium SZBI oraz komunikowane wszystkim właściwym osobom ze szczególnym uwzględnieniem nowych obowiązków lub zmian narzędzi.

9.5 Nowo zatrudnione osoby muszą zostać zapoznane z aktualną wersją polityki w ramach wdrożenia. Wszyscy pracownicy muszą ukończyć szkolenie przypominające po istotnych zmianach polityki.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest bezpośrednio wspierana przez środki kontrolne opisane w następujących powiązanych politykach i wymusza ich stosowanie:

10.1.1 P4 - Polityka kontroli dostępu: dostęp do informacji jest regulowany przez poziomy klasyfikacji; dane bardziej wrażliwe wymagają bardziej rygorystycznej kontroli dostępu i mechanizmów autoryzacji.

10.1.2 P11 - Polityka zarządzania kontami użytkowników i uprawnieniami: wzmacnia przydzielanie uprawnień zgodnie z zasadą wiedzy koniecznej, wynikającą z poziomów klasyfikacji.

10.1.3 P12 - Polityka zarządzania aktywami: zapewnia, że każde aktywo ujęte w inwentarzu zawiera swoją klasyfikację i oznaczenie, wspierając identyfikowalność i rozliczalność.

10.1.4 P14 - Polityka retencji danych i utylizacji: zasady utylizacji i przechowywania są określane na podstawie poziomu klasyfikacji danych oraz regulacyjnych wymogów retencji.

10.1.5 P18 - Polityka zabezpieczeń kryptograficznych: stosuje odpowiednie standardy szyfrowania w zależności od klasyfikacji aktywa informacyjnego.

10.1.6 P22 - Polityka rejestrowania i monitorowania: umożliwia monitorowanie dostępu do informacji sklasyfikowanych i ich przepływu, zapewniając możliwość śledzenia na potrzeby audytu oraz wykrywanie błędnego oznaczania lub niewłaściwego użycia.

10.2 Każde z tych powiązań zapewnia spójną ochronę informacji w całym ich cyklu życia — od utworzenia i klasyfikacji po bezpieczne postępowanie, przechowywanie, transmisję i ostateczne zniszczenie.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z uznanymi międzynarodowo normami i ramami regulacyjnymi dotyczącymi klasyfikacji i oznaczania informacji wrażliwych.

11.2 ISO/IEC 27001

11.2.1 Klauzula 4.2 - Zrozumienie potrzeb i oczekiwań stron zainteresowanych. Wymagania dotyczące klasyfikacji często wynikają z obowiązków prawnych, regulacyjnych lub umownych nakładanych przez strony zainteresowane (np. RODO, umowy o zachowaniu poufności z klientami), co musi zostać odzwierciedlone w polityce.

11.2.2 Klauzula 6.1.3 - Postępowanie z ryzykiem w bezpieczeństwie informacji. Klasyfikacja bezpośrednio wpływa na dobór środków postępowania z ryzykiem, w tym kontroli dostępu, szyfrowania i przechowywania, w zależności od wrażliwości danych.

11.2.3 Klauzula 7.2 - Kompetencje. Polityka wymaga, aby personel odpowiedzialny za klasyfikację i oznaczanie był przeszkolony, co mieści się w wymaganiach dotyczących kompetencji.

11.2.4 Klauzula 7.3 - Świadomość. Polityka wymaga, aby wszyscy użytkownicy byli świadomi poziomów klasyfikacji i swoich obowiązków w zakresie postępowania z informacjami, co jest zgodne z wymaganiami dotyczącymi świadomości.

11.2.5 Klauzula 7.5 - Udokumentowane informacje. Sama polityka klasyfikacji jest dokumentem nadzorowanym, a procedury, zapisy szkoleniowe i oznaczenia klasyfikacyjne stanowią część udokumentowanych informacji.

11.2.6 Klauzula 8.1 - Planowanie operacyjne i nadzór. Klasyfikacja i oznaczanie to procesy operacyjne osadzone w zarządzaniu cyklem życia danych, a niniejsza klauzula zapewnia, że działania te są planowane, wdrażane i nadzorowane.

11.2.7 Klauzula 9.1 - Monitorowanie, pomiary, analiza i ocena. Polityka zawiera postanowienia dotyczące monitorowania zgodności klasyfikacji, trendów incydentów oraz skuteczności schematu oznaczania.

11.2.8 Klauzula 10.1 - Niezgodność i działanie korygujące. Polityka określa reakcje na błędną klasyfikację, w tym działania korygujące, takie jak ponowne szkolenie, aktualizacje i obsługa odstępstw.

11.3 ISO/IEC 27002:2022

11.3.1 Środek kontrolny 5.12 - Klasyfikacja informacji. Ten środek kontrolny zapewnia klasyfikację informacji na podstawie ich wrażliwości, wartości i krytyczności — dokładnie to formalizuje niniejsza polityka.

11.3.2 Środek kontrolny 5.13 - Oznaczanie informacji. Ten środek kontrolny wymaga odpowiedniego oznaczania informacji zgodnie z ich poziomem klasyfikacji, co zostało w pełni ujęte w polityce.

11.3.3 Środek kontrolny 5.10 - Dopuszczalne użytkowanie aktywów organizacji. Polityka określa sposób postępowania użytkowników z danymi sklasyfikowanymi, bezpośrednio wspierając dopuszczalne użytkowanie aktywów organizacji i zapobiegając niewłaściwemu użyciu.

11.3.4 Środek kontrolny 5.11 - Zwrot aktywów. Klasyfikacja pomaga zapewnić identyfikację danych wrażliwych oraz ich bezpieczny zwrot lub sanityzację przy odejściu pracownika lub dostawcy.

11.3.5 Środek kontrolny 5.9 - Inwentarz aktywów informacyjnych i innych powiązanych aktywów. Klasyfikacja jest często powiązana z inwentarzem aktywów, który musi odzwierciedlać poziom klasyfikacji każdego elementu, aby wspierać właściwy dobór środków kontrolnych.

11.3.6 Środek kontrolny 5.14 - Przekazywanie informacji. Poziomy klasyfikacji wpływają na środki kontrolne dotyczące wewnętrznego i zewnętrznego transferu danych (np. szyfrowanie, zatwierdzanie, ograniczenia dostępu).

11.3.7 Środek kontrolny 8.12 - Zapobieganie wyciekom danych. Egzekwowanie klasyfikacji i oznaczania wspiera zapobieganie nieuprawnionemu ujawnieniu i utracie danych.

11.3.8 Środek kontrolny 8.11 - Maskowanie danych. Niektóre poziomy klasyfikacji (np. Poufne, Zastrzeżone) mogą wymagać maskowania, gdy dane są używane w środowiskach testowych i rozwojowych lub do analiz.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Polityka i procedury ochrony systemów i komunikacji: wspiera polityki klasyfikacji jako element nadrzędnej ochrony danych.

11.4.2 AC-16 - Atrybuty bezpieczeństwa: wdraża wymuszanie dostępu na podstawie metadanych klasyfikacyjnych i uprawnień użytkownika.

11.4.3 MP-3 / MP-5 - Oznaczanie nośników i ochrona transportu: wymusza oznaczanie i ochronę danych podczas przechowywania i transmisji zgodnie z klasyfikacją.

11.5 RODO (2016/679)

11.5.1 Artykuł 5 - Zasady ochrony danych: wymaga, aby dane osobowe były przetwarzane w sposób bezpieczny i proporcjonalny do ich wrażliwości.

11.5.2 Artykuł 32 - Bezpieczeństwo przetwarzania: wzmacnia klasyfikację jako mechanizm ochrony danych oparty na ryzyku oraz wspierający dobór właściwych środków technicznych.

11.6 Dyrektywa UE NIS2 (2022/2555)

11.6.1 Artykuł 21(2)(a): wymaga polityk dotyczących zarządzania ryzykiem w bezpieczeństwie informacji, w tym środków kontroli klasyfikacji aktywów i danych.

11.6.2 Artykuł 21(3): wspiera stosowanie środków zapewniających właściwe postępowanie z danymi — realizowane poprzez oznaczanie oparte na klasyfikacji.

11.7 Rozporządzenie UE DORA (2022/2554)

11.7.1 Artykuł 5 - Ład zarządczy i kontrola: wymaga ram ładu zarządczego klasyfikujących aktywa danych na potrzeby kontroli ryzyka ICT.

11.7.2 Artykuł 9 - Zarządzanie ryzykiem ICT: nakłada obowiązek stosowania środków technicznych i organizacyjnych wobec krytycznych aktywów ICT, w tym klasyfikacji i oznaczania.

11.8 COBIT 2019

11.8.1 DSS05.02 - Zarządzanie usługami bezpieczeństwa: egzekwuje klasyfikację bezpieczeństwa informacji w celu zapewnienia ochrony danych przedsiębiorstwa.

11.8.2 MEA03 - Monitorowanie, ocena i weryfikacja zgodności: wspiera regularny audyt i przegląd praktyk klasyfikacji w celu zapewnienia przestrzegania polityki oraz dojrzałości procesu.