					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P13S					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**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 5.3, 8	
ISO/IEC 27002:2022	Środki kontrolne 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
Dyrektywa NIS2 UE	Artykuł 21(2)(a)	
Rozporządzenie DORA UE	Artykuł 5(8)	
COBIT 2019	BAI03.05, DSS05	
RODO	Artykuł 5, 32	

1. Cel

1.1 Niniejsza polityka określa sposób klasyfikowania i oznaczania wszystkich informacji przetwarzanych przez organizację w celu zapewnienia poufności, integralności i dostępności tych informacji w całym cyklu życia.

1.2 Zapewnia spójne postępowanie z danymi poprzez przypisanie odpowiednich poziomów ochrony do informacji na podstawie ich wrażliwości, wpływu na działalność biznesową lub obowiązków prawnych.

1.3 Klasyfikacja i oznaczanie pomagają ograniczać ryzyko przypadkowego ujawnienia, nieuprawnionego dostępu lub niewłaściwego postępowania z danymi wrażliwymi, zwłaszcza w organizacjach typu SME, które mogą opierać się na prostszych systemach i mniejszej liczbie sformalizowanych zabezpieczeń.

1.4 Niniejsza polityka ma istotne znaczenie dla certyfikacji ISO/IEC 27001 oraz zgodności z wymaganiami regulacyjnymi, w szczególności z przepisami o ochronie danych, takimi jak RODO, oraz z ramami cyberbezpieczeństwa, takimi jak NIS2 i DORA.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich danych organizacji, niezależnie od ich formatu lub lokalizacji, w tym do:

2.1.1 dokumentów elektronicznych, arkuszy kalkulacyjnych, wiadomości e-mail, formularzy, obrazów i zeskanowanych plików,

2.1.2 dokumentów w postaci papierowej, takich jak wydruki, raporty, faktury i notatki,

2.1.3 danych przechowywanych lub przetwarzanych w usługach chmurowych, na serwerach lokalnych, nośnikach wymiennych lub urządzeniach prywatnych wykorzystywanych do celów służbowych,

2.1.4 danych tymczasowych lub przejściowych generowanych w trakcie operacji biznesowych (np. logów, plików pamięci podręcznej, wiadomości e-mail).

2.2 Wszyscy pracownicy, wykonawcy, pracownicy tymczasowi oraz dostawcy zewnętrzni posiadający dostęp do danych organizacji są zobowiązani do przestrzegania niniejszej polityki.

2.3 Polityka ma zastosowanie do całego cyklu życia danych — od ich utworzenia i przechowywania, przez dostęp i transfer, aż po archiwizację lub usunięcie.

3. Cele

3.1 Zdefiniowanie prostego i egzekwowalnego schematu klasyfikacji, który może być łatwo zrozumiany i stosowany w całej organizacji.

3.2 Wymaganie, aby każdy zasób danych był klasyfikowany zgodnie ze swoją wrażliwością i odpowiednio oznaczany w celu zapewnienia właściwego postępowania, przechowywania i dostępu.

3.3 Zapewnienie, że praktyki oznaczania danych są zintegrowane z procesami biznesowymi, takimi jak wdrożenia, uruchamianie projektów i konfiguracja systemów.

3.4 Ograniczenie ryzyka naruszeń poprzez stosowanie zabezpieczeń związanych z postępowaniem z danymi (np. szyfrowania, ograniczeń dostępu) zgodnie z poziomem klasyfikacji.

3.5 Zapewnienie zgodności z przepisami dotyczącymi prywatności danych i bezpieczeństwa informacji poprzez wykazanie, że dane wrażliwe (np. dane osobowe, finansowe lub zastrzeżone) są prawidłowo oznaczane i zarządzane.

3.6 Ustanowienie rozliczalności za decyzje klasyfikacyjne oraz zapewnienie okresowych przeglądów i aktualizacji w oparciu o zmieniające się potrzeby biznesowe i prawne.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Jest właścicielem niniejszej polityki i zatwierdza schemat klasyfikacji.

4.1.2 Sprawuje nadzór, aby zapewnić delegowanie i egzekwowanie odpowiedzialności związanych z klasyfikacją.

4.1.3 Dokonuje przeglądu i zatwierdza wszelkie odstępstwa od wymagań dotyczących klasyfikacji lub oznaczania.

4.1.4 Zapewnia, że praktyki postępowania z danymi spełniają wymagania zgodności wynikające z przepisów, takich jak RODO i DORA.

4.2 Właściciel informacji / Menedżer danych

4.2.1 Nadaje wstępną klasyfikację każdemu nowemu zbiorowi danych lub aktywu informacyjnemu w momencie jego utworzenia lub pozyskania.

4.2.2 Zapewnia stosowanie widocznych oznaczeń (np. nagłówków plików, stopek, znaków wodnych, nazw folderów), tam gdzie ma to zastosowanie.

4.2.3 Dokonuje okresowego przeglądu klasyfikacji w celu potwierdzenia jej aktualności, poprawności oraz ewentualnej potrzeby zmiany (np. po obniżeniu klasyfikacji lub publikacji).

4.2.4 Współpracuje z osobą odpowiedzialną za IT w celu egzekwowania zabezpieczeń technicznych zgodnie z klasyfikacją (np. praw dostępu, szyfrowania).

[... 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 corocznemu przeglądowi przez GM oraz Menedżera danych w celu zapewnienia, że odzwierciedla ona:

9.1.1 zmiany w działalności biznesowej lub rodzajach danych,

9.1.2 nowe wymagania regulacyjne (np. dotyczące prywatności danych lub nadzoru finansowego),

9.1.3 zmiany technologiczne wpływające na możliwości oznaczania lub klasyfikacji.

9.2 Przegląd musi obejmować aktualizacje kategorii klasyfikacji, narzędzi lub praktyk oznaczania oraz treści dotyczących świadomości i szkoleń.

9.3 Zmiany polityki muszą zostać zatwierdzone przez GM i zakomunikowane całemu personelowi. Historia wersji musi być przechowywana na potrzeby audytu.

10. Powiązane polityki i zależności

10.1 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: przypisuje rozliczalność za własność polityki i stosowanie jej postanowień.

10.2 P4S – Polityka kontroli dostępu: zapewnia zgodność dostępu do systemów z poziomami klasyfikacji danych.

10.3 P12S – Polityka zarządzania aktywami: zapewnia ewidencję aktywów fizycznych i cyfrowych przechowujących dane sklasyfikowane.

10.4 P17S – Polityka ochrony danych i prywatności: reguluje ochronę danych osobowych, z których znaczna część jest klasyfikowana jako Poufne.

10.5 P30S – Polityka reagowania na incydenty: określa ścieżki eskalacji i procedury reagowania w przypadku naruszeń klasyfikacji lub ujawnienia danych.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 5.3: wymaga jednoznacznego zdefiniowania odpowiedzialności za postępowanie z danymi i ich ochronę.

11.1.2 Klauzula 8.1: wymaga planowania operacyjnego i stosowania zabezpieczeń, w tym powiązanych z klasyfikacją danych.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 5.12: zawiera wytyczne dotyczące klasyfikacji informacji na podstawie ryzyka i wymagań regulacyjnych.

11.2.2 Środek kontrolny 5.13: określa praktyczne mechanizmy oznaczania oraz powiązane zasady postępowania.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: wymaga oznaczania informacji w celu zapewnienia, że zabezpieczenia są zgodne z klasyfikacją.

11.3.2 MP-3 / MP-5: zawierają wytyczne dotyczące oznaczania i kontroli nośników oraz danych wyjściowych.

11.4 RODO

11.4.1 Artykuły 5 i 32: wymagają minimalizacji danych oraz zapewnienia integralności poprzez właściwą klasyfikację i odpowiednie zabezpieczenia.

11.5 NIS2

11.5.1 Artykuł 21(2)(a): wymaga stosowania zabezpieczeń technicznych i organizacyjnych dla ochrony danych opartej na ryzyku.

11.6 DORA

11.6.1 Artykuł 5(8): wymaga od organizacji klasyfikowania aktywów danych jako części programu zarządzania ryzykiem ICT.

11.7 COBIT 2019

11.7.1 BAI03.05: wymaga klasyfikacji informacji i stosowania ochrony dostosowanej do ryzyka.

11.7.2 DSS05.02: odnosi się do egzekwowania zabezpieczeń opartych na klasyfikacji oraz monitorowania.