					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P14					Tytuł dokumentu: **Polityka retencji i utylizacji danych**							
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 6.1.3, 8.1	
ISO/IEC 27002:2022	Środki kontrolne 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
RODO	Artykuły 5(1)(e), 17, 32	
Dyrektywa NIS2	Artykuł 21(2)(a-e)	
Rozporządzenie DORA	Artykuły 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Cel

1.1 Celem niniejszej polityki jest określenie wymagań organizacyjnych dotyczących retencji danych i ich bezpiecznej utylizacji na wszystkich etapach cyklu życia informacji. Polityka zapewnia zgodność z mającymi zastosowanie wymaganiami prawnymi, regulacyjnymi i umownymi oraz zapobiega niepotrzebnemu lub ryzykownemu gromadzeniu danych.

1.2 Niniejsza polityka wspiera wdrożenie normy ISO/IEC 27001:2022 poprzez egzekwowanie kontroli nad okresami przechowywania danych oraz stosowanie nieodwracalnych metod utylizacji. Umożliwia prowadzenie dokumentacji w sposób zapewniający ścieżkę audytu, wymusza okresy przechowywania adekwatne do klasyfikacji informacji oraz zapewnia gotowość do audytu, kontroli regulacyjnej i postępowania dowodowego.

1.3 Polityka ma również na celu utrzymanie poufności, integralności i dostępności (CIA) danych przy jednoczesnym ograniczaniu ryzyka biznesowego, nieefektywności operacyjnych oraz ekspozycji na naruszenia prywatności wynikające z niewłaściwej retencji lub niszczenia danych.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich fizycznych i cyfrowych aktywów informacyjnych będących własnością organizacji, przetwarzanych przez organizację lub przechowywanych przez organizację, w tym pozostających pod kontrolą stron trzecich, spółek zależnych lub partnerów świadczących usługi outsourcingowe.

2.2 Zakres obejmuje między innymi:

2.2.1 dokumenty, pliki i zapisy (w formie cyfrowej i papierowej),

2.2.2 bazy danych i archiwa,

2.2.3 wiadomości e-mail i logi komunikatorów,

2.2.4 kopie zapasowe, logi systemowe i ścieżki audytu,

2.2.5 kod źródłowy, dane aplikacyjne i zasoby hostowane w chmurze,

2.2.6 nośniki wymienne oraz wycofany sprzęt zawierający dane.

2.3 Polityka reguluje zarówno zapisy operacyjne, jak i zbiory danych podlegające regulacjom (np. dane finansowe, prawne, kadrowe, dotyczące klientów i istotne z perspektywy audytu), niezależnie od lokalizacji przechowywania lub systemu.

2.4 Ma ona zastosowanie do wszystkich jednostek organizacyjnych oraz do wszystkich pracowników, kontraktorów i dostawców zaangażowanych w tworzenie, przechowywanie, zarządzanie lub utylizację danych.

3. Cele

3.1 Zapewnienie, że dane są przechowywane wyłącznie przez okres wymagany prawnie, umownie lub operacyjnie, a po ustaniu tej potrzeby są bezpiecznie utylizowane.

3.2 Zapobieganie przedwczesnemu, nieuprawnionemu lub przypadkowemu usunięciu zapisów wymaganych do bieżącej działalności, zapewnienia zgodności, postępowań spornych lub celów audytowych.

3.3 Ustanowienie i egzekwowanie spójnych harmonogramów retencji opartych na klasyfikacji informacji, typie aktywów, mających zastosowanie przepisach prawa oraz ekspozycji na ryzyko.

3.4 Ochrona prywatności i poufności danych w okresie ich przechowywania oraz w momencie utylizacji, w tym realizacja praw osób, których dane dotyczą (np. usunięcie danych zgodnie z art. 17 RODO).

3.5 Zapewnienie, że wszystkie metody utylizacji danych są nieodwracalne, odpowiednio udokumentowane i zgodne z uznanymi standardami, takimi jak NIST SP 800-88.

3.6 Ograniczenie nieefektywności operacyjnych, nadmiernych kosztów i ekspozycji prawnej spowodowanych zbyt długim przechowywaniem danych lub nieobjętymi nadzorem danymi historycznymi.

3.7 Wspieranie celów ciągłości działania i odtwarzania po awarii poprzez zintegrowany nadzór nad retencją kopii zapasowych oraz stosowanie dających się obronić praktyk archiwizacji danych.

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze

4.1.1 Zatwierdza niniejszą politykę oraz zapewnia odpowiednie finansowanie, zasoby i integrację z programami zarządzania ryzykiem korporacyjnym i zgodnością.

4.1.2 Ponosi ogólną odpowiedzialność za zgodność z wymaganiami prawnymi i regulacyjnymi w zakresie retencji danych i bezpiecznej utylizacji.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO)

4.2.1 Jest właścicielem niniejszej polityki i odpowiada za definiowanie oraz przegląd zasad zarządzania retencją i utylizacją zgodnie z SZBI.

4.2.2 Zapewnia wdrożenie wymagań dotyczących retencji i utylizacji opartych na klasyfikacji w jednostkach biznesowych i systemach technicznych.

4.2.3 Monitoruje zgodność z polityką i inicjuje działania korygujące, gdy jest to konieczne.

[... 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 podlega przeglądowi raz w roku lub w przypadku wystąpienia któregokolwiek z poniższych warunków:

9.1.1 zmian w mających zastosowanie przepisach prawa lub regulacjach wpływających na retencję danych (np. aktualizacje RODO, przepisów podatkowych, DORA),

9.1.2 zmian w ramach klasyfikacji lub procesach biznesowych wpływających na etapy cyklu życia danych,

9.1.3 wdrożenia nowych systemów IT, platform archiwizacyjnych lub technologii utylizacji nośników,

9.1.4 ustaleń audytu wewnętrznego lub zaleceń regulacyjnych wskazujących luki w praktykach retencji lub utylizacji.

9.2 Przegląd prowadzą CISO oraz Inspektor Ochrony Danych (IOD), przy udziale działu prawnego, funkcji zgodności, IT oraz jednostek biznesowych.

9.3 Główny harmonogram retencji danych (MDRS) oraz Rejestr utylizacji muszą być przeglądane równolegle, aby zapewnić, że:

9.3.1 harmonogramy pozostają prawidłowe i odzwierciedlają potrzeby operacyjne, prawne i regulacyjne,

9.3.2 dokumentacja utylizacji jest kompletna i zapewnia ścieżkę audytu,

9.3.3 zapisy blokady prawnej są walidowane i zwalniane, gdy jest to właściwe.

9.4 Wszelkie aktualizacje polityki muszą:

9.4.1 podlegać formalnemu wersjonowaniu i być przechowywane w repozytorium dokumentów SZBI,

9.4.2 zawierać historię wersji i uzasadnienie zmiany,

9.4.3 być zatwierdzone przez kierownictwo wykonawcze,

9.4.4 zostać zakomunikowane odpowiedniemu personelowi wraz ze zaktualizowanymi materiałami szkoleniowymi lub wytycznymi.

9.5 W przypadku istotnych zmian polityki pracownicy, których to dotyczy, muszą ukończyć ukierunkowane szkolenie w ciągu 30 dni od publikacji, aby zapewnić dalszą zgodność.

9.6 Polityki powiązane i zależności

10. Polityki powiązane i zależności

10.1.1 P4 - Polityka kontroli dostępu: zapewnia, że w okresie retencji do danych mają dostęp wyłącznie osoby upoważnione, a dane po upływie okresu przechowywania są objęte ograniczeniami do czasu utylizacji.

10.1.2 P12 - Polityka zarządzania aktywami: identyfikuje aktywa zawierające dane wymagające planowej utylizacji oraz śledzi ich cykl życia od pozyskania do zniszczenia.

10.1.3 P13 - Polityka klasyfikacji i oznaczania danych: stanowi podstawę decyzji klasyfikacyjnych, które bezpośrednio wpływają na okres przechowywania danych oraz wymaganą metodę utylizacji.

10.1.4 P15 - Polityka kopii zapasowych i odtwarzania: definiuje okresy retencji i procedury utylizacji dla nośników kopii zapasowych oraz replikowanych zasobów danych.

10.1.5 P18 - Polityka zabezpieczeń kryptograficznych: wspiera usunięcie kryptograficzne na potrzeby utylizacji oraz wymusza szyfrowanie danych przechowywanych do momentu zniszczenia.

10.1.6 P30 - Polityka reagowania na incydenty: jest uruchamiana w przypadkach, gdy niewłaściwa utylizacja skutkuje potencjalną utratą danych, naruszeniem bezpieczeństwa lub naruszeniem wymagań regulacyjnych.

10.2 Każda z polityk powiązanych odgrywa rolę we wdrożeniu spójnego modelu zarządzania danymi w obszarach klasyfikacji, kontroli cyklu życia, dostępu oraz gotowości audytowej.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z uznanymi na świecie normami i ramami regulacyjnymi określającymi bezpieczne, zgodne i efektywne praktyki zarządzania cyklem życia danych.

11.2 ISO/IEC 27001:

11.2.1 Klauzula 6.1.3 - plan postępowania z ryzykiem: wspiera ograniczanie ryzyk związanych z nadmierną retencją, naruszeniami danych lub nieskutecznością utylizacji.

11.2.2 Klauzula 8.1 - planowanie i nadzór operacyjny: ustanawia mechanizmy kontroli cyklu życia regulujące przechowywanie, archiwizację i niszczenie.

11.3 ISO/IEC 27002:2022 - środki kontrolne 5.10, 5.12, 5.30, 5: dostarczają praktycznych wytycznych dotyczących dopuszczalnego użytkowania aktywów organizacji, zasadności retencji, kontrolowanego usuwania oraz możliwego do obrony prowadzenia zapisów zgodnie z tolerancją ryzyka organizacji.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - przechowywanie zapisów audytowych: zapewnia wystarczający okres przechowywania logów audytowych i dowodów zgodności.

11.4.2 MP-6 - sanitacja nośników: wymaga bezpiecznych, udokumentowanych metod niszczenia nośników fizycznych i elektronicznych.

11.4.3 SI-12 - postępowanie z informacją: wymusza odpowiednie postępowanie z danymi zgodnie z mechanizmami kontroli retencji i utylizacji.

11.4.4 PL-2 - plan bezpieczeństwa i prywatności systemu: wymaga dokumentacji specyficznej dla systemu w zakresie postępowania z danymi w cyklu życia oraz postanowień dotyczących bezpiecznej utylizacji.

11.5 RODO (2016/679):

11.5.1 Artykuł 5(1)(e) - minimalizacja danych i ograniczenie przechowywania: wymaga, aby dane nie były przechowywane dłużej, niż jest to konieczne.

11.5.2 Artykuł 17 - prawo do usunięcia danych („prawo do bycia zapomnianym”): wymaga niezwłocznego i trwałego usunięcia danych osobowych na podstawie ważnego żądania.

11.5.3 Artykuł 32 - bezpieczeństwo przetwarzania: wzmacnia ochronę danych w okresie przechowywania i wymaga bezpiecznego niszczenia zapisów, dla których upłynął okres przechowywania.

11.6 Dyrektywa NIS2 (2022/2555):

11.6.1 Artykuł 21(2)(a-e): wymaga, aby podmioty przyjmowały polityki i środki techniczne w zakresie bezpiecznego postępowania z danymi, w tym ograniczeń przechowywania i metod utylizacji.

11.7 Rozporządzenie DORA (2022/2554):

11.7.1 Artykuł 5 - ład zarządczy i kontrola: nakłada obowiązek stosowania ustrukturyzowanego zarządzania ryzykiem ICT, w tym bezpiecznego postępowania z informacją w całym cyklu życia.

11.7.2 Artykuł 9 - ramy zarządzania ryzykiem ICT: wymaga polityk dotyczących retencji danych, niszczenia danych oraz zgodności prawnej i regulacyjnej operacji cyfrowych.

11.8 COBIT 2019:

11.8.1 DSS01 - zarządzane operacje: wspiera śledzenie retencji i spójność pomiędzy systemami danych.

11.8.2 DSS05 - zarządzane usługi bezpieczeństwa: zapewnia ochronę danych przechowywanych i archiwizowanych do czasu bezpiecznej utylizacji.

11.8.3 MEA03 - monitorowanie, ocena i ocena zgodności: umożliwia audytowanie egzekwowania retencji, procedur usuwania i realizacji wymagań regulacyjnych.