					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P14S					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**

Nota prawna (prawa autorskie i ograniczenia użytkowania)

(C) 2025 Clarysec LLC. All rights reserved.

Niniejszy dokument stanowi własność intelektualną spółki Clarysec LLC. Żadna część tego dokumentu nie może być kopiowana, ponownie wykorzystywana, rozpowszechniana ani modyfikowana do celów komercyjnych lub wdrożeniowych bez uprzedniej wyraźnej pisemnej zgody.
Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych.
W sprawach licencjonowania prosimy o kontakt: info@clarysec.com

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 6.1.3, 8	Obejmuje postępowanie z ryzykiem, operacyjne środki bezpieczeństwa oraz wymagania dotyczące okresów przechowywania
ISO/IEC 27002:2022	Środek kontrolny 5	Wytyczne dotyczące okresów przechowywania i metod bezpiecznego niszczenia
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12	Okresy przechowywania zapisów audytowych, sanityzacja nośników, limity retencji danych i ich egzekwowanie
Dyrektywa NIS2	Artykuł 21(2)(a)	Wymagana polityka zarządzania cyklem życia adekwatna do ryzyka
Rozporządzenie DORA	Artykuł 5(1)	Zarządzanie ryzykiem ICT: dostępność i usuwanie danych
RODO	Artykuł 5(1)(e), 17	Dane nie mogą być przechowywane dłużej, niż jest to niezbędne; prawo do usunięcia
COBIT 2019	BAI03.04, DSS01	Kontrole cyklu życia informacji, bezpieczna utylizacja

1. Cel

1.1 Celem niniejszej polityki jest określenie wiążących zasad retencji i bezpiecznej utylizacji informacji w środowisku SME. Zapewnia ona, że zapisy są przechowywane wyłącznie przez okres wymagany przepisami prawa, zobowiązaniami umownymi lub uzasadnioną potrzebą biznesową, a następnie bezpiecznie niszczone.

1.2 Niniejsza polityka ma na celu ograniczenie ryzyka informacyjnego, zarządzanie ekspozycją prawną oraz zmniejszenie skali przechowywania danych zbędnych lub nieaktualnych. Wspiera zapewnienie zgodności z ISO/IEC 27001 oraz ramami ochrony prywatności, takimi jak RODO, poprzez ograniczanie nieuprawnionego przechowywania danych osobowych lub informacji wrażliwych.

1.3 Dobrze ustrukturyzowane zasady retencji i utylizacji ograniczają koszty operacyjne, poprawiają wydajność systemów oraz zwiększają gotowość audytową. W przypadku organizacji SME o ograniczonych zasobach IT zapewniają praktyczny sposób odpowiedzialnego zarządzania cyfrowymi i fizycznymi aktywami informacyjnymi.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich zapisów, plików, dzienników, komunikacji i zbiorów danych tworzonych, gromadzonych, przetwarzanych lub przechowywanych przez organizację;

2.1.2 wszystkich pracowników, kontraktorów i dostawców zewnętrznych przetwarzających dane organizacji;

2.1.3 wszystkich formatów danych (np. papierowych, elektronicznych, obrazów, nagrań audio lub dzienników) oraz wszystkich nośników przechowywania (np. dysków lokalnych, usług chmurowych, serwerów poczty elektronicznej, kopii zapasowych).

2.2 Zakres obejmuje:

2.2.1 dokumenty biznesowe (np. faktury, umowy, raporty projektowe);

2.2.2 zapisy operacyjne (np. dzienniki, historię dostępu, migawki kopii zapasowych);

2.2.3 dane osobowe (np. akta HR, komunikację z klientami, zapisy wsparcia);

2.2.4 dane hostowane wewnętrznie, zewnętrznie lub w systemach hybrydowych;

2.2.5 dane archiwalne i dane z kopii zapasowych, niezależnie od tego, czy są aktywne, czy nieaktywne.

2.3 Zakres obejmuje wszystkie etapy cyklu życia danych — od ich utworzenia do autoryzowanej utylizacji.

3. Cele

3.1 Ustanowienie spójnych zasad retencji na podstawie kryteriów prawnych, operacyjnych i regulacyjnych.

3.2 Zapobieganie przedwczesnemu usuwaniu krytycznych zapisów oraz eliminowanie zbędnej akumulacji danych.

3.3 Zapewnienie bezpiecznej i nieodwracalnej utylizacji danych, gdy ich przechowywanie nie jest już wymagane.

3.4 Przypisanie odpowiedzialności za egzekwowanie decyzji dotyczących retencji i usuwania z uwzględnieniem ograniczeń kadrowych typowych dla organizacji SME.

3.5 Zapewnienie dokumentacji gotowej do audytu w celu wykazania należytej staranności zgodnie z ISO/IEC 27001, RODO, NIS2 i innymi ramami.

3.6 Wspieranie bezpiecznego postępowania z danymi w całym cyklu życia bez nakładania nadmiernych obciążeń technicznych na personel niespecjalistyczny.

4. Role i obowiązki

4.1 Dyrektor Generalny (GM)

4.1.1 Zatwierdza niniejszą politykę i ponosi za nią odpowiedzialność.

4.1.2 Zapewnia wdrożenie procedur retencji i utylizacji w sposób adekwatny do ryzyka prawnego i biznesowego.

4.1.3 W razie potrzeby zatwierdza odstępstwa oraz zastosowanie zabezpieczenia prawnego i wstrzymania usuwania.

4.1.4 Inicjuje przeglądy polityki i zatwierdza aktualizacje wynikające ze zmian biznesowych lub regulacyjnych.

4.2 Wyznaczony właściciel danych

4.2.1 Jest wyznaczany dla każdej kategorii danych (np. danych finansowych, HR, zapisów klientów).

4.2.2 Klasyfikuje zapisy i określa odpowiedni okres przechowywania na podstawie polityki oraz wytycznych prawnych.

4.2.3 Autoryzuje usunięcie po spełnieniu wymagań dotyczących retencji.

4.2.4 Wspiera audyty wewnętrzne, dostarczając kontekst dotyczący zasad retencji i zdarzeń utylizacji.

[... 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 przeglądana co najmniej raz w roku lub w przypadku:

9.1.1 zmian w mających zastosowanie przepisach prawa (np. dotyczących ochrony prywatności danych, sprawozdawczości finansowej);

9.1.2 wdrożenia nowych systemów lub procesów wpływających na cykl życia danych;

9.1.3 ustaleń audytowych lub incydentów ujawniających luki w praktykach retencji.

9.2 Przeglądy muszą zapewniać, że Rejestr retencji pozostaje kompletny i odzwierciedla wszystkie główne kategorie zapisów.

9.3 Aktualizacje polityki muszą być zatwierdzane przez GM i komunikowane odpowiedniemu personelowi. Najnowsza wersja musi być dostępna i objęta kontrolą wersji.

10. Powiązane polityki i zależności

10.1 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: określa właściciela polityki oraz uprawnienia do zatwierdzania odstępstw.

10.2 P13S – Polityka klasyfikacji i etykietowania danych: określa sposób powiązania zasad retencji z klasyfikacją danych.

10.3 P12S – Polityka zarządzania aktywami: reguluje zasady dotyczące nośników przechowujących dane objęte retencją i utylizacją.

10.4 P17S – Polityka ochrony danych i prywatności: zapewnia minimalizację danych i wspiera zgodne z prawem przetwarzanie informacji zgodnie z RODO.

10.5 P30S – Polityka reagowania na incydenty: ma zastosowanie, gdy nieskuteczna utylizacja lub retencja prowadzi do potencjalnego ujawnienia danych.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 6.1.3: wymaga postępowania z ryzykami związanymi z informacją, w tym z ryzykami retencji.

11.1.2 Klauzula 8.1: określa operacyjne środki kontroli cyklu życia.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 5.33: wytyczne dotyczące ustalania okresów przechowywania i metod bezpiecznego niszczenia.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: wymagany okres przechowywania zapisów audytowych.

11.3.2 MP-6: określa procedury sanityzacji nośników.

11.3.3 SI-12: dotyczy limitów retencji danych i ich egzekwowania.

11.4 RODO

11.4.1 Artykuł 5(1)(e): dane muszą być przechowywane nie dłużej, niż jest to niezbędne.

11.4.2 Artykuł 17: prawo do usunięcia ma zastosowanie, gdy dane nie są już zgodnie z prawem przechowywane.

11.5 NIS2

11.5.1 Artykuł 21(2)(a): wymaga stosowania polityk organizacyjnych adekwatnych do ryzyka, w tym zarządzania cyklem życia.

11.6 DORA

11.6.1 Artykuł 5(1): zarządzanie ryzykiem ICT obejmuje dostępność i usuwanie danych.

11.7 COBIT 2019

11.7.1 BAI03.04: wymagane są kontrole cyklu życia informacji.

11.7.2 DSS01.06: procedury bezpiecznej utylizacji jako element ochrony aktywów informacyjnych.