					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P01S					Tytuł dokumentu: **Polityka 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	Klauzule 5.1, 5.2, 5.3, 6.1, 6.2, 8	Określa zaangażowanie kierownictwa, wymagania dotyczące polityki, przypisanie ról, ocenę ryzyka oraz nadzór operacyjny
ISO/IEC 27002:2022	Środki kontrolne 5.1–5.5	Określa ustanawianie udokumentowanych polityk bezpieczeństwa informacji, przypisanie ról, rozdzielenie obowiązków oraz odpowiedzialność kierownictwa
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Określa wymagania dotyczące planu programu bezpieczeństwa, polityki planowania, oceny i autoryzacji oraz kontroli dostępu
RODO (2016/679)	Artykuł 5 ust. 2, Artykuł 32	Ustanawia zasadę rozliczalności oraz wymagania dotyczące bezpieczeństwa przetwarzania, w szczególności w zakresie udokumentowanych ról
Dyrektywa NIS2 (2022/2555)	Artykuł 21 ust. 2 lit. a	Wymaga środków zarządzania ryzykiem, ról i odpowiedzialności w obszarze cyberbezpieczeństwa
Rozporządzenie DORA (2022/2554)	Artykuł 9, Artykuł 10	Wymaga przypisania ról w zakresie zarządzania ryzykiem ICT i ciągłości działania
COBIT 2019	EDM03, APO13, DSS05	Wspiera optymalizację ryzyka, zarządzanie bezpieczeństwem oraz zarządzanie usługami bezpieczeństwa poprzez jednoznaczne przypisanie ról

1. Cel

1.1 Niniejsza polityka potwierdza zaangażowanie organizacji w ochronę informacji klientów i informacji biznesowych poprzez jednoznaczne określenie odpowiedzialności oraz praktycznych środków bezpieczeństwa, odpowiednich dla organizacji nieposiadających dedykowanych zespołów IT.

1.2 Zapewnia, że wszyscy pracownicy, współpracownicy i dostawcy usług przestrzegają obowiązujących zasad, umożliwiających pełną zgodność z wymaganiami certyfikacji ISO/IEC 27001.

1.3 Niniejsza polityka umożliwia organizacji budowanie zaufania klientów poprzez jednoznaczne wykazanie, w jaki sposób chronione są ich informacje dzięki zdefiniowanym odpowiedzialnościom, uporządkowanym procesom oraz silnej rozliczalności.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich osób, które uzyskują dostęp do danych i systemów organizacji lub nimi zarządzają, w tym:

2.1.1 właścicieli biznesowych i Dyrektora Generalnego

2.1.2 pracowników, współpracowników i stażystów

2.1.3 zewnętrznych dostawców wsparcia IT lub konsultantów

2.2 Obejmuje wszystkie rodzaje informacji, systemów i usług, w tym:

2.2.1 dokumentację biznesową, dane klientów, hasła i wiadomości e-mail

2.2.2 sprzęt IT, taki jak laptopy i telefony

2.2.3 usługi chmurowe wykorzystywane do przechowywania plików, komunikacji lub finansów

2.2.4 dokumenty papierowe przechowywane w lokalizacjach biurowych

2.3 Polityka obowiązuje we wszystkich środowiskach pracy — biurowych, zdalnych i chmurowych — oraz obejmuje wszystkie urządzenia i oprogramowanie wykorzystywane do przetwarzania lub przechowywania informacji biznesowych.

3. Cele

3.1 Jednoznaczne przypisanie odpowiedzialności: należy zapewnić, aby za bezpieczeństwo informacji zawsze odpowiadała konkretna osoba. Co do zasady jest to Dyrektor Generalny lub osoba formalnie przez niego wyznaczona.

3.2 Ochrona informacji klientów i informacji biznesowych: należy zapewnić niezawodne i spójne środki bezpieczeństwa zapobiegające niewłaściwemu wykorzystaniu, utracie lub kradzieży danych wrażliwych, w tym danych klientów i dokumentacji finansowej.

3.3 Wsparcie certyfikacji ISO/IEC 27001: należy umożliwić organizacji wykazanie pełnej zgodności z wymaganiami ISO/IEC 27001, zapewniając gotowość do audytu i możliwość uzyskania certyfikacji bez konieczności wdrażania złożonej infrastruktury.

3.4 Włączenie bezpieczeństwa do działalności operacyjnej: należy zintegrować bezpieczeństwo informacji z codziennymi zadaniami i decyzjami w całej organizacji.

3.5 Budowanie świadomości i kultury bezpieczeństwa: należy zapewnić, aby każdy pracownik rozumiał i stosował praktyki bezpieczeństwa, takie jak używanie silnych haseł i zgłaszanie podejrzanych działań.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny lub właściciel biznesowy

4.1.1 Ponosi pełną odpowiedzialność za bezpieczeństwo informacji.

4.1.2 Zatwierdza niniejszą politykę i odpowiada za jej utrzymanie.

4.1.3 Zapewnia, że wszystkie kluczowe zadania związane z bezpieczeństwem są realizowane bezpośrednio albo delegowane na piśmie.

4.1.4 Weryfikuje, że wszelkie delegowane zadania związane z bezpieczeństwem (takie jak zarządzanie dostępem lub reagowanie na incydenty) są wykonywane skutecznie.

4.1.5 Pełni funkcję domyślnego punktu kontaktowego we wszystkich wewnętrznych i zewnętrznych sprawach związanych z bezpieczeństwem, w tym podczas audytów i w odpowiedzi na zapytania klientów.

4.1.6 Monitoruje realizację tych celów podczas corocznego przeglądu. Cele powinny być mierzalne tam, gdzie jest to możliwe (np. odsetek przeszkolonego personelu, liczba zgłoszonych incydentów itp.) oraz aktualizowane na podstawie ustaleń bezpieczeństwa i zmian poziomu ryzyka.

4.2 Wyznaczony pracownik (jeżeli dotyczy)

4.2.1 Może wspierać Dyrektora Generalnego w realizacji codziennych zadań, takich jak tworzenie kont użytkowników, odbieranie uprawnień osobom kończącym współpracę lub koordynacja działań z dostawcą wsparcia IT.

4.2.2 Musi być formalnie wyznaczony oraz posiadać wystarczające uprawnienia i narzędzia do realizacji powierzonych zadań.

4.2.3 Zgłasza wszelkie problemy Dyrektorowi Generalnemu.

[... 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 Coroczny przegląd

9.1.1 Niniejsza polityka musi być przeglądana przez Dyrektora Generalnego (GM) co najmniej raz w roku w celu zapewnienia ciągłej zgodności z wymaganiami certyfikacji ISO/IEC 27001, zmianami regulacyjnymi (takimi jak RODO, NIS2 i DORA) oraz zmieniającymi się potrzebami biznesowymi.

9.2 Przeglądy doraźne

9.2.1 Dodatkowe przeglądy muszą być przeprowadzane zawsze, gdy wystąpią istotne zmiany, takie jak:

9.2.1.1 poważne incydenty bezpieczeństwa lub naruszenia

9.2.1.2 wdrożenie nowych procesów biznesowych lub technologii (np. nowego oprogramowania, platform pracy zdalnej lub usług chmurowych)

9.2.1.3 zmiany wymagań prawnych lub regulacyjnych wpływających na postępowanie z informacjami

9.3 Dokumentowanie zmian

9.3.1 Wszystkie przeglądy polityki oraz zmiany muszą być formalnie dokumentowane, z jednoznacznym wskazaniem daty, charakteru zmian oraz zatwierdzenia przez GM.

9.3.2 Historyczny rejestr wersji polityki musi być bezpiecznie utrzymywany w celu wykazania ewolucji polityki i zgodności podczas audytów.

9.4 Komunikowanie aktualizacji

9.4.1 Wszelkie zmiany niniejszej polityki muszą być niezwłocznie komunikowane wszystkim pracownikom, współpracownikom i odpowiednim stronom trzecim.

9.4.2 Zaktualizowane wersje polityki muszą być łatwo dostępne dla całego personelu, którego dotyczą (np. udostępnione elektronicznie lub wywieszone fizycznie w miejscu pracy).

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest ściśle powiązana z innymi politykami w zestawie polityk SME organizacji, w szczególności:

10.1.1 P2S – Polityka ról i odpowiedzialności w zakresie ładu zarządczego: doprecyzowuje przypisanie obowiązków i odpowiedzialności w zakresie bezpieczeństwa.

10.1.2 P4S – Polityka kontroli dostępu: określa zasady bezpiecznego zarządzania dostępem do informacji organizacji.

10.1.3 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zawiera podstawowe wytyczne dotyczące szkoleń i budowania świadomości personelu.

10.1.4 P17S – Polityka ochrony danych i prywatności: zapewnia zgodność z RODO oraz innymi przepisami dotyczącymi ochrony danych.

10.1.5 P30S – Polityka reagowania na incydenty: opisuje szczegółowe działania wymagane w odpowiedzi na incydenty bezpieczeństwa.

10.2 Te powiązane polityki zapewniają jednoznaczne wytyczne operacyjne i muszą być wdrażane łącznie, aby osiągnąć pełną zgodność z wymaganiami certyfikacji ISO/IEC 27001.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 5.1 – Przywództwo i zaangażowanie: wymaga zaangażowania najwyższego kierownictwa oraz odpowiedzialności za skuteczność bezpieczeństwa informacji w organizacji.

11.1.2 Klauzula 5.2 – Polityka bezpieczeństwa informacji: nakłada obowiązek ustanowienia jasnych, udokumentowanych polityk zgodnych ze strategią organizacji i wymaganiami zgodności.

11.1.3 Klauzula 5.3 – Role organizacyjne i odpowiedzialności: określa jednoznaczne przypisanie odpowiedzialności za bezpieczeństwo informacji w całej organizacji, co jest niezbędne dla skutecznego ładu zarządczego i zgodności audytowej.

11.1.4 Klauzula 6.1 – Działania dotyczące ryzyk i szans: zapewnia systematyczną identyfikację, ocenę i postępowanie z ryzykami dla bezpieczeństwa informacji.

11.1.5 Klauzula 8.1 – Planowanie i nadzór operacyjny: wymaga, aby organizacja planowała i wdrażała procesy niezbędne do osiągania celów bezpieczeństwa informacji oraz skutecznego zarządzania związanymi z nimi ryzykami.

11.2 Środki kontrolne ISO/IEC 27002:2022 5.1–5.5

11.2.1 Załącznik A, Środek kontrolny 5.1 – Polityki bezpieczeństwa informacji: określa ustanawianie i komunikowanie udokumentowanych polityk bezpieczeństwa informacji.

11.2.2 Załącznik A, Środek kontrolny 5.2 – Role bezpieczeństwa informacji: doprecyzowuje i formalnie przypisuje role i odpowiedzialności w zakresie bezpieczeństwa informacji odpowiednim stronom.

11.2.3 Załącznik A, Środek kontrolny 5.3 – Rozdzielenie obowiązków: wymaga jednoznacznego rozdzielenia obowiązków w celu ograniczenia konfliktów interesów i ryzyka nadużyć przy zarządzaniu informacjami wrażliwymi.

11.2.4 Załącznik A, Środek kontrolny 5.4 – Odpowiedzialność kierownictwa: wymaga, aby kierownictwo wykazywało zaangażowanie w bezpieczeństwo informacji poprzez aktywny nadzór i alokację zasobów.

11.2.5 Wzmacnia konieczność jednoznacznie udokumentowanych polityk bezpieczeństwa informacji, ról, odpowiedzialności i struktur ładu zarządczego, zapewniając spójne zarządzanie oraz możliwość prześledzenia działań podczas audytu w całej organizacji.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plan programu bezpieczeństwa informacji: wymaga udokumentowanych strategii i polityk ładu zarządczego bezpieczeństwa informacji, zapewniających ramy dla spójnego wdrożenia i zarządzania.

11.3.2 PL-1 – Polityka planowania bezpieczeństwa: nakłada obowiązek ustanowienia ogólnoorganizacyjnej polityki planowania bezpieczeństwa w celu ukierunkowania bezpiecznej eksploatacji oraz strategicznego dostosowania działań w obszarze bezpieczeństwa informacji.

11.3.3 CA-1 – Polityka oceny i autoryzacji bezpieczeństwa: wymaga jednoznacznie określonych ról w zakresie oceny i autoryzacji, aby zapewnić ciągłą skuteczność oraz zgodność z wymaganiami bezpieczeństwa informacji.

11.3.4 AC-1 – Polityka kontroli dostępu: wymaga od organizacji jednoznacznego określenia, udokumentowania i stosowania praktyk oraz odpowiedzialności związanych z zarządzaniem dostępem.

11.4 RODO (2016/679)

11.4.1 Artykuł 5 ust. 2 – Zasada rozliczalności: wymaga od organizacji wykazania zgodności z zasadami ochrony danych, w tym posiadania udokumentowanych ról i polityk dotyczących odpowiedzialności za ochronę danych.

11.4.2 Artykuł 32 – Bezpieczeństwo przetwarzania: nakłada obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, w tym jasno określonych odpowiedzialności za

bezpieczeństwo, w celu ochrony danych osobowych przed naruszeniami i nieuprawnionym dostępem.

11.5 Dyrektywa NIS2 (2022/2555)

11.5.1 Artykuł 21 ust. 2 lit. a – Środki zarządzania ryzykiem: wymaga jasnych rozwiązań w zakresie ładu zarządczego, w tym określonych ról i odpowiedzialności w obszarze bezpieczeństwa informacji, niezbędnych do skutecznego zarządzania ryzykiem cyberbezpieczeństwa.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 9 – Zarządzanie ryzykiem ICT: wymaga, aby organizacje jednoznacznie przypisywały role i odpowiedzialności związane z zarządzaniem ryzykiem ICT, wzmacniając odporność i gotowość do zapewnienia ciągłości działania.

11.6.2 Artykuł 10 – Ciągłość działania ICT: wymaga jednoznacznej odpowiedzialności i uporządkowanych ról dla utrzymania odporności i ciągłości ICT, zapewniając organizacjom zdolność do niezawodnego reagowania na zakłócenia.

11.7 COBIT 2019

11.7.1 EDM03 – Zapewnienie optymalizacji ryzyka: podkreśla znaczenie jednoznacznie określonej odpowiedzialności i ról w zarządzaniu ryzykami organizacyjnymi, zapewniając silny ład zarządczy i skuteczny nadzór nad ryzykami bezpieczeństwa informacji.

11.7.2 APO13 – Zarządzanie bezpieczeństwem: wymaga, aby organizacje jednoznacznie ustanawiały i komunikowały odpowiedzialności za zarządzanie bezpieczeństwem, zapewniając zgodność z celami biznesowymi i wymaganiami regulacyjnymi.

11.7.3 DSS05 – Zarządzanie usługami bezpieczeństwa: wskazuje na potrzebę uporządkowanych ról i jednoznacznych odpowiedzialności w zarządzaniu usługami bezpieczeństwa, umożliwiając spójne wdrożenie i weryfikację zgodności.