					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P01					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**

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

1. Cel

1.1 Niniejsza polityka określa nadrzędne zobowiązanie organizacji w zakresie bezpieczeństwa informacji poprzez ustanowienie formalnego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

1.2 Wyznacza kierunek strategiczny oraz podstawowe wymagania dotyczące ochrony poufności, integralności, dostępności i odporności wszystkich aktywów informacyjnych w środowiskach fizycznych, cyfrowych i chmurowych.

1.3 Polityka realizuje wymagania klauzul 5.1 i 5.2 normy ISO/IEC 27001:2022, określając intencje przywódcze, zaangażowanie najwyższego kierownictwa oraz powiązanie działań w zakresie bezpieczeństwa z celami organizacji.

1.4 Stanowi wiążący punkt odniesienia dla wszystkich polityk podrzędnych, standardów i procedur w ramach SZBI oraz ma kluczowe znaczenie dla zapewnienia środowiska bezpieczeństwa opartego na ryzyku, zgodności i ciągłym doskonaleniu.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich osób, aktywów i procesów zdefiniowanych w zakresie SZBI, w tym do:

2.1.1 wszystkich jednostek biznesowych, działów, spółek zależnych i oddziałów

2.1.2 pracowników, wykonawców, personelu tymczasowego, konsultantów oraz dostawców usług zewnętrznych

2.1.3 wszystkich danych, systemów informatycznych, aplikacji, infrastruktury i kanałów komunikacji

2.1.4 wszystkich środowisk fizycznych, chmurowych, zdalnych i hybrydowych, w których dane organizacji są przetwarzane lub do których uzyskuje się dostęp

2.2 Polityka jest wiążąca dla wszystkich podmiotów przetwarzających informacje organizacji i obejmuje wszystkie etapy cyklu życia informacji — od utworzenia i transmisji po przechowywanie i utylizację.

2.3 Wszelkie wyłączenia lub ograniczenia tego zakresu muszą być udokumentowane w Deklaracji zakresu SZBI i uzasadnione formalną akceptacją kierownictwa wykonawczego.

3. Cele

3.1 Ustanowienie SZBI zgodnego z ISO/IEC 27001:2022 i wspierającego podejmowanie decyzji w oparciu o ryzyko w całej organizacji.

3.2 Zapewnienie, aby zasady bezpieczeństwa dotyczące poufności, integralności i dostępności były wbudowane we wszystkie działania organizacji, systemy i relacje partnerskie.

3.3 Zapewnienie zgodności regulacyjnej oraz zgodności z wymaganiami umownymi poprzez określenie mierzalnych celów bezpieczeństwa wynikających z polityk i zintegrowanie ich z działalnością operacyjną.

3.4 Ograniczenie prawdopodobieństwa wystąpienia i wpływu incydentów bezpieczeństwa informacji poprzez skuteczne zabezpieczenia zapobiegawcze, detekcyjne i korygujące.

3.5 Wspieranie ciągłego doskonalenia dojrzałości bezpieczeństwa informacji poprzez określone wskaźniki efektywności, wyniki audytów oraz przeglądy zarządzania SZBI.

3.6 Promowanie kultury rozliczalności, świadomości i odporności, w której obowiązki w zakresie bezpieczeństwa są rozumiane i realizowane przez cały personel.

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze

4.1.1 Zatwierdza i przyjmuje Politykę bezpieczeństwa informacji oraz ramy SZBI.

4.1.2 Zapewnia spójność pomiędzy celami bezpieczeństwa a strategią biznesową.

4.1.3 Daje przykład i promuje silną kulturę bezpieczeństwa informacji.

4.1.4 Dokonuje przeglądu i zatwierdza istotne zmiany zakresu SZBI, postępowania z ryzykiem i struktury ładu zarządczego.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO) / Menedżer Systemu Zarządzania Bezpieczeństwem Informacji

4.2.1 Odpowiada za SZBI i utrzymuje niniejszą politykę zgodnie z ISO/IEC 27001.

4.2.2 Kieruje procesami oceny ryzyka, wdrażania zabezpieczeń i ciągłego doskonalenia.

4.2.3 Zapewnia międzyfunkcyjną koordynację działań w zakresie bezpieczeństwa oraz nadzoruje polityki podrzędne.

4.2.4 Raportuje najwyższemu kierownictwu status SZBI, incydenty, wyniki audytów i wskaźniki.

4.2.5 Zapewnia przeprowadzanie przeglądów i aktualizacji polityki zgodnie z sekcją 9 niniejszego dokumentu.

[... 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 Częstotliwość przeglądu

9.1.1 Niniejsza polityka musi podlegać przeglądowi co najmniej raz w roku lub po wystąpieniu któregokolwiek z następujących zdarzeń:

9.1.1.1 istotnych zmian obowiązków prawnych, regulacyjnych lub umownych

9.1.1.2 istotnych zmian w profilu ryzyka organizacji

9.1.1.3 wyników audytów wewnętrznych lub zewnętrznych

9.1.1.4 poważnych incydentów lub nieskuteczności zabezpieczeń

9.2 Uprawnienia i proces przeglądu

9.2.1 Dyrektor ds. bezpieczeństwa informacji (CISO) lub wyznaczony Menedżer Systemu Zarządzania Bezpieczeństwem Informacji kieruje procesem przeglądu.

9.2.2 Dane wejściowe do przeglądu muszą obejmować:

9.2.2.1 wyniki audytów wewnętrznych

9.2.2.2 trendy ocen ryzyka

9.2.2.3 zmiany procesów biznesowych i technologii

9.2.2.4 wyniki względem KPI i progów ryzyka

9.2.3 Wszystkie aktualizacje muszą:

9.2.3.1 podlegać kontroli wersji i zostać udokumentowane

9.2.3.2 zostać zatwierdzone przez kierownictwo wykonawcze

9.2.3.3 zostać przekazane wszystkim zainteresowanym stronom za pośrednictwem oficjalnych kanałów komunikacji

9.2.3.4 skutkować odpowiednimi aktualizacjami dokumentacji podrzędnej i szkoleń

10. Powiązane polityki i zależności

10.1 Niniejsza polityka nadrzędna jest bezpośrednio powiązana z następującymi politykami bezpieczeństwa i ramami organizacyjnymi:

10.1.1 P2 – Polityka ról i odpowiedzialności w zakresie ładu zarządczego: określa strukturę ładu zarządczego i hierarchię uprawnień, do których odwołuje się niniejszy dokument.

10.1.2 P3 – Polityka dopuszczalnego użytkowania: określa wymagania dotyczące zachowań oraz dopuszczalnego postępowania z aktywami informacyjnymi.

10.1.3 P4 – Polityka kontroli dostępu: operacjonalizuje zabezpieczenia związane z dostępem wynikające z niniejszej polityki nadrzędnej.

10.1.4 P6 – Polityka zarządzania ryzykiem: zapewnia kontekst oparty na ryzyku dla doboru zabezpieczeń i akceptacji ryzyka rezydualnego.

10.1.5 P33 – Polityka audytu i monitorowania zgodności: określa, w jaki sposób wewnętrzne mechanizmy zapewnienia potwierdzają stosowanie polityki.

10.2 Te współzależności zapewniają kompleksowe dopasowanie i możliwość prześledzenia w całym SZBI oraz wspierają spójny ład zarządzania ryzykiem i zgodnością.

11. Normy i ramy odniesienia

11.1 Niniejsza Polityka bezpieczeństwa informacji jest formalnie zgodna z następującymi normami i ramami, aby zapewnić pełną zgodność, gotowość do audytu oraz możliwość obrony w przypadku kontroli regulacyjnej:

11.2 ISO/IEC 27001

11.2.1 Klauzula 5.1 – Przywództwo i zaangażowanie: niniejsza polityka potwierdza zaangażowanie najwyższego kierownictwa w bezpieczeństwo informacji oraz określa odpowiedzialności i alokację zasobów dla SZBI.

11.2.2 Klauzula 5.2 – Polityka bezpieczeństwa informacji: niniejszy dokument stanowi formalną politykę bezpieczeństwa organizacji, zgodną z określonymi celami bezpieczeństwa, strategią biznesową oraz wymaganiami ISO/IEC 27001.

11.2.3 Klauzula 6.1 – Działania odnoszące się do ryzyk i szans: podejście oparte na ryzyku odzwierciedlone w niniejszej polityce zapewnia proporcjonalne stosowanie zasobów bezpieczeństwa do zagrożeń.

11.2.4 Klauzula 9.2 – Audyt wewnętrzny oraz klauzula 10 – Doskonalenie: niniejsza polityka jest osadzona w cyklu ciągłego doskonalenia organizacji i podlega walidacji w ramach audytu wewnętrznego.

11.2.5 ISO/IEC 27002:2022 – Środek kontrolny 5.1: określa wytyczne dotyczące ustanawiania i utrzymywania polityk bezpieczeństwa. Niniejsza polityka odzwierciedla zalecenia ISO/IEC 27002 w zakresie hierarchii dokumentacji, cykli przeglądu oraz stosowalności.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Polityka i procedury planowania bezpieczeństwa): niniejsza polityka spełnia wymaganie opracowania, rozpowszechnienia i przeglądu formalnej, obowiązującej w całej organizacji polityki bezpieczeństwa informacji.

11.3.2 PM-1 do PM-5: obejmuje ład na poziomie programu, w tym role w obszarze bezpieczeństwa informacji, alokację zasobów, strategię ryzyka oraz integrację planowania bezpieczeństwa z operacjami organizacji.

11.4 RODO (2016/679)

11.4.1 Artykuł 5(2): egzekwuje zasadę rozliczalności. Niniejsza polityka określa strony odpowiedzialne oraz działania audytowalne.

11.4.2 Artykuł 24: wymaga wdrożenia środków technicznych i organizacyjnych, w tym polityk zgodnych z ryzykiem.

11.4.3 Artykuł 32: wspiera wdrożenie odpowiednich środków w celu zapewnienia bezpieczeństwa danych osobowych w całym ich cyklu życia.

11.5 Dyrektywa NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(a): nakłada na podmioty obowiązek wdrożenia udokumentowanej polityki bezpieczeństwa obejmującej zarządzanie ryzykiem i ład zarządczy. Niniejsza polityka spełnia ten wymóg oraz wspiera szerszą gotowość w zakresie cyberbezpieczeństwa i ochronę infrastruktury krytycznej.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 5(2): wymaga udokumentowanych ram kontroli wewnętrznej dla zarządzania ryzykiem ICT. Niniejsza polityka wspiera zgodność sektora finansowego poprzez przypisanie ról, zabezpieczeń i funkcji nadzorczych zgodnie z oczekiwaniami DORA w zakresie ładu zarządczego.

11.7 COBIT 2019

11.7.1 EDM01 – Ustanowienie ram ładu zarządczego: niniejsza polityka wspiera ład organizacyjny poprzez określenie ról SZBI, zobowiązań przywódczych i celów strategicznych.

11.7.2 APO01 – Ramy zarządzania: wspiera ustanowienie i funkcjonowanie uporządkowanego SZBI.

11.7.3 APO12 – Zarządzanie ryzykiem: zapewnia podstawę dla ładu zarządzania ryzykiem bezpieczeństwa informacji.

11.7.4 MEA01/MEA03 – Monitorowanie, ocena i weryfikacja: wzmacnia ciągłą ocenę efektywności i monitorowanie kontroli wewnętrznej poprzez egzekwowanie zgodności z polityką.