					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P18					Tytuł dokumentu: **Polityka zabezpieczeń kryptograficznych**							
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	Klauzula 8	-
ISO/IEC 27002:2022	Środki kontrolne 8.24, 8.25, 8	-
NIST SP 800-53 Rev. 5	SC-12 do SC-17, SC-28, SC-28(1), SC-12(3)	-
RODO	Artykuł 32, Artykuły 33–34, Motyw 83	-
Dyrektywa NIS2	Artykuł 21(2)(d)	-
Rozporządzenie DORA	Artykuły 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA03	-

1. Cel

1.1 Niniejsza polityka określa obowiązkowe wymagania dotyczące bezpiecznego i zgodnego z wymaganiami stosowania zabezpieczeń kryptograficznych w całej organizacji, w celu zapewnienia poufności, integralności i autentyczności informacji wrażliwych i regulowanych.

1.2 Stosowanie kryptografii stanowi podstawę zaufania do operacji związanych z bezpieczeństwem danych, wspiera bezpieczną komunikację, wymusza kontrolę dostępu oraz umożliwia zapewnienie zgodności regulacyjnej poprzez skuteczne szyfrowanie i właściwe praktyki zarządzania kluczami.

1.3 Niniejsza polityka jest zgodna z ISO/IEC 27001:2022, klauzulą 8.1 oraz Załącznikiem A, środkiem kontrolnym 8.24, a także wspiera obowiązki prawne i operacyjne wynikające z art. 32 RODO, art. 6(2)(d) DORA oraz art. 21 NIS2. Wspiera również cele COBIT 2019 w zakresie usług bezpieczeństwa i ochrony aktywów informacyjnych.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich jednostek organizacyjnych, funkcji biznesowych, członków personelu oraz dostawców usług zewnętrznych zaangażowanych w stosowanie, administrowanie lub wdrażanie narzędzi i metod kryptograficznych.

2.2 Zakres obejmuje środowiska produkcyjne, rozwojowe, testowe, systemy kopii zapasowych oraz środowiska odtwarzania po awarii, w których dane wrażliwe są przesyłane, przetwarzane lub przechowywane.

2.3 Zakres obejmuje wszystkie komponenty kryptograficzne i przypadki użycia, w tym między innymi:

2.3.1 szyfrowanie symetryczne i asymetryczne

2.3.2 podpisy cyfrowe i certyfikaty

2.3.3 algorytmy haszujące

2.3.4 bezpieczne generowanie, dystrybucję i niszczenie kluczy

2.3.5 zabezpieczenia warstwy transportowej (TLS), szyfrowanie pełnodyskowe oraz szyfrowanie na poziomie interfejsów API

2.3.6 bezpieczne komponenty, takie jak moduły bezpieczeństwa sprzętowego (HSM), moduły zaufanej platformy (TPM) oraz systemy zarządzania kluczami (KMS)

2.4 Niniejsza polityka reguluje stosowanie kryptografii w odniesieniu do:

2.4.1 danych sklasyfikowanych jako Poufne, Wysoce poufne lub Regulowane

2.4.2 uwierzytelniania i weryfikacji tożsamości cyfrowych

2.4.3 bezpiecznej komunikacji ze stronami zewnętrznymi

2.4.4 pieczy nad kluczami i mechanizmów podwójnej kontroli

3. Cele

3.1 Należy zapewnić, aby technologie kryptograficzne były dobierane, zatwierdzane, wdrażane i utrzymywane zgodnie z ryzykiem biznesowym, normami międzynarodowymi oraz wymogami regulacyjnymi.

3.2 Należy ustanowić ustandaryzowaną strukturę ładu zarządczego dla zarządzania usługami kryptograficznymi, obejmującą jednoznaczną rozliczalność za wdrożenie, walidację i obsługę odstępstw.

3.3 Należy zapobiegać nieuprawnionemu stosowaniu, błędnej konfiguracji lub dezaktualizacji algorytmów kryptograficznych i zabezpieczeń kryptograficznych poprzez formalny proces zatwierdzania i przeglądu.

3.4 Należy zapewnić, aby zabezpieczenia kryptograficzne były uwzględniane na etapie projektowania systemów i regularnie walidowane w celu zapobiegania ujawnieniu danych, kompromitacji kluczy lub osłabieniu protokołów.

3.5 Należy wymagać zarządzania cyklem życia wszystkich kluczy kryptograficznych, w tym ich generowania, przechowywania, użycia, rotacji, unieważniania i bezpiecznego niszczenia.

3.6 Należy zapewnić zgodność z międzynarodowymi i regionalnymi regulacjami wymagającymi szyfrowania i bezpiecznego postępowania z danymi, w tym z RODO, DORA, NIS2 i COBIT 2019.

4. Role i odpowiedzialności

4.1 Menedżer ds. bezpieczeństwa informacji / Dyrektor ds. bezpieczeństwa informacji (CISO)

4.1.1 Jest właścicielem niniejszej polityki i zapewnia jej zgodność z Systemem Zarządzania Bezpieczeństwem Informacji (SZBI) oraz Załącznikiem A do ISO/IEC 27001, środkiem kontrolnym 8.24.

4.1.2 Zatwierdza stosowanie algorytmów kryptograficznych i zabezpieczeń kryptograficznych oraz zapewnia przestrzeganie niniejszej polityki w całej organizacji.

4.2 Kierownik operacji kryptograficznych / Architekt bezpieczeństwa

4.2.1 Zarządza bieżącymi operacjami i administrowaniem systemami kryptograficznymi.

4.2.2 Utrzymuje wykaz zatwierdzonych metod kryptograficznych (ACML) oraz Rejestr zarządzania kluczami.

4.2.3 Prowadzi przeglądy projektów kryptograficznych (CDR) oraz ocenia nowe technologie kryptograficzne.

[... 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 corocznemu przeglądowi przez Menedżera ds. bezpieczeństwa informacji oraz kierownika operacji kryptograficznych.

9.2 Przesłanki przeglądu obejmują:

9.2.1 wykrycie podatności kryptograficznych (np. obniżenie poziomu bezpieczeństwa algorytmu, ataki kwantowe)

9.2.2 zmiany regulacyjne wymagające aktualizacji standardów szyfrowania

9.2.3 ustalenia operacyjne lub audytowe ujawniające luki w polityce

9.2.4 aktualizacje narzędzi kryptograficznych lub zmiany architektoniczne

9.3 Aktualizacje muszą podlegać kontroli wersji w Rejestrze dokumentów SZBI i być komunikowane do:

9.3.1 wszystkich administratorów posiadających role z dostępem kryptograficznym

9.3.2 zespołów rozwojowych i liderów DevSecOps

9.3.3 dostawców zewnętrznych objętych umownymi zobowiązaniami w zakresie szyfrowania

9.4 Zespół SZBI musi zapewnić archiwizację wersji zastąpionych oraz zaprzestanie ich przywoływania w procedurach operacyjnych.

10. Powiązane polityki i zależności

10.1 P1 - Polityka bezpieczeństwa informacji. Zapewnia podstawy ładu zarządczego dla wszystkich środków bezpieczeństwa, w tym stosowania zabezpieczeń kryptograficznych, ochrony aktywów oraz bezpiecznej komunikacji.

10.2 P4 - Polityka kontroli dostępu. Zapewnia, że dostęp logiczny do materiału kryptograficznego i systemów zarządzania szyfrowaniem jest ściśle ograniczony zgodnie z zasadą najmniejszych uprawnień oraz rozdzieleniem obowiązków.

10.3 P6 - Polityka zarządzania ryzykiem. Wspiera ocenę ryzyk związanych z zabezpieczeniami kryptograficznymi oraz dokumentuje strategię postępowania z ryzykiem dla odstępstw, dezaktualizacji algorytmów lub scenariuszy kompromitacji kluczy.

10.4 P12 - Polityka zarządzania aktywami. Wymaga klasyfikacji danych wrażliwych i aktywów sprzętowych, co bezpośrednio determinuje wymagania kryptograficzne oraz obowiązki związane z pieczą nad kluczami.

10.5 P13 - Polityka klasyfikacji danych i etykietowania. Definiuje poziomy klasyfikacji (np. Poufne, Regulowane), które uruchamiają określone wymagania szyfrowania w tranzycie i w spoczynku.

10.6 P14 - Polityka retencji danych i utylizacji. Określa procedury bezpiecznej utylizacji zaszyfrowanych nośników danych oraz materiału kluczy kryptograficznych po zakończeniu cyklu życia.

10.7 P30 - Polityka reagowania na incydenty (P30). Określa strategię reakcji organizacji na kompromitację kluczy, niewłaściwe użycie certyfikatów lub podejrzenie podatności algorytmicznych, w tym szybkie unieważnienie oraz zgłaszanie naruszeń.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 - planowanie i nadzór operacyjny: wymaga stosowania technicznych środków bezpieczeństwa, w tym zabezpieczeń kryptograficznych, jako elementu zabezpieczeń operacyjnych.

11.2 ISO/IEC 27002:2022

11.2.1 Środki kontrolne 8.24, 8.25, 8: zawierają wytyczne wdrożeniowe dotyczące celów zabezpieczeń kryptograficznych, doboru algorytmów, wymuszania protokołów oraz zarządzania cyklem życia certyfikatów.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 - ustanawianie kluczy kryptograficznych: zapewnia bezpieczne generowanie i wymianę kluczy szyfrowania. P18 określa, w jaki sposób klucze symetryczne i asymetryczne muszą być generowane i wymieniane z użyciem zatwierdzonych algorytmów i protokołów.

11.3.2 SC-13 - ochrona kryptograficzna: wymaga stosowania kryptografii do ochrony poufności i integralności informacji. P18 wymusza szyfrowanie danych w spoczynku i w tranzycie na podstawie klasyfikacji danych, przy zachowaniu standardów algorytmów zgodnych z NIST FIPS 140-3.

11.3.3 SC-17 - certyfikaty infrastruktury klucza publicznego (PKI): wymaga wdrożenia PKI w celu wsparcia uwierzytelniania i podpisów cyfrowych. P18 określa zastosowanie PKI do zabezpieczania komunikacji, tożsamości systemowych i dostępu administracyjnego.

11.3.4 SC-28, SC-28(1) - ochrona informacji w spoczynku i w tranzycie: wymaga szyfrowania danych przechowywanych lub przesyłanych przez niezaufane sieci. P18 określa wymuszanie TLS, tuneli VPN, szyfrowania pełnodyskowego oraz bezpiecznych metod przechowywania danych wrażliwych.

11.3.5 SC-12(3) - generowanie kluczy symetrycznych do bezpiecznego przechowywania i dystrybucji: koncentruje się na bezpiecznym generowaniu i obsłudze kluczy symetrycznych. P18 wymaga stosowania silnych generatorów liczb losowych, zasad rotacji kluczy oraz bezpiecznych repozytoriów kluczy na potrzeby operacji kryptograficznych.

11.4 RODO (2016/679)

11.4.1 Artykuł 32 - bezpieczeństwo przetwarzania: wprost zaleca szyfrowanie jako środek redukcji ryzyka dla danych osobowych.

11.4.2 Motyw 83: podkreśla szyfrowanie jako mechanizm zapobiegający nieuprawnionemu dostępowi do danych.

11.4.3 Artykuły 33 i 34: skuteczne szyfrowanie może zwolnić organizację z obowiązku notyfikacji naruszenia w określonych przypadkach.

11.5 Dyrektywa NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(d): wymaga środków technicznych i organizacyjnych, w tym ochrony kryptograficznej, w celu utrzymania dostępności i integralności usług.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 6(2)(d): instytucje finansowe muszą zabezpieczać dane, w tym poprzez silne szyfrowanie informacji krytycznych.

11.6.2 Artykuł 11(1)(c): wymaga bezpiecznych mechanizmów przetwarzania danych dla dostawców usług ICT będących stroną trzecią.

11.7 COBIT 2019

11.7.1 DSS05.01 - ochrona aktywów informacyjnych: wymaga stosowania szyfrowania i zarządzania kluczami w celu ochrony danych przed nieuprawnionym dostępem.

11.7.2 DSS06.06 - zarządzane testowanie bezpieczeństwa: zaleca walidację zgodności kryptograficznej jako część ocen podatności.

11.7.3 MEA03 - monitorowanie, ocena i przegląd zgodności: wymaga ciągłego zapewnienia skuteczności zabezpieczeń kryptograficznych.