					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P31					Tytuł dokumentu: **Polityka zabezpieczania materiału dowodowego i informatyki śledczej**							
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 kontroli 5.25–5.27, 8.27	
ISO/IEC 27035:2016	Części 1 i 3	
NIST SP 800-53 Rev. 5	IR-1 do IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Informatyka śledcza urządzeń mobilnych i nośników	Informatyka śledcza urządzeń mobilnych i nośników
NIST SP 800-86	Integracja technik śledczych	Integracja technik śledczych z reagowaniem na incydenty
RODO	Artykuł 5, 33–34	
Dyrektywa NIS2	Artykuł 23(1)–(4)	
Rozporządzenie DORA	Artykuł 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Cel

1.1 Niniejsza polityka ustanawia uporządkowane i prawnie defensywne ramy identyfikacji, pozyskiwania, zabezpieczania, analizy i utylizacji dowodów cyfrowych w trakcie rzeczywistych lub podejrzewanych incydentów bezpieczeństwa.

1.2 Polityka zapewnia, że procesy gotowości śledczej i postępowania z materiałem dowodowym:

1.2.1 Zachowują integralność materiału dowodowego oraz łańcuch nadzoru

1.2.2 Wspierają dochodzenia wewnętrzne, postępowania prawne lub raportowanie regulacyjne

1.2.3 Są zgodne z międzynarodowo uznanymi standardami informatyki śledczej oraz kryteriami dopuszczalności dowodowej

1.3 Polityka wspiera zobowiązanie organizacji do proaktywnego reagowania na incydenty, zgodności z przepisami oraz przejrzystości ładu korporacyjnego, przy jednoczesnym ograniczaniu zakłóceń operacyjnych.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich pracowników, wykonawców, dostawców oraz usługodawców zaangażowanych w administrowanie systemami, obsługę incydentów lub czynności dochodzeniowe

2.1.2 wszystkich punktów końcowych, serwerów, aplikacji, sieci oraz platform chmurowych pozostających pod kontrolą organizacji lub objętych jej odpowiedzialnością umowną

2.1.3 każdego incydentu lub zdarzenia wymagającego postępowania z materiałem dowodowym, w tym:

2.1.3.1 zagrożeń wewnętrznych, naruszeń ochrony danych lub dochodzeń dotyczących oszustw

2.1.3.2 niewłaściwego użycia systemów lub poświadczeń

2.1.3.3 incydentów związanych z technologią operacyjną (OT) lub systemami sterowania przemysłowego

2.1.3.4 naruszeń dostępu fizycznego dotyczących aktywów cyfrowych

2.2 Polityka reguluje również wszelkie interakcje z zewnętrznymi dostawcami usług informatyki śledczej lub organami ścigania w ramach eskalacji prawnych lub postępowań regulacyjnych.

3. Cele

3.1 Umożliwienie szybkiego, bezpiecznego i zgodnego z polityką pozyskiwania materiału dowodowego podczas zdarzeń bezpieczeństwa informacji lub dochodzeń.

3.2 Zachowanie integralności, autentyczności i dopuszczalności zgromadzonych dowodów cyfrowych poprzez ścisłą kontrolę dostępu, rejestrowanie oraz procedury weryfikacji.

3.3 Zapewnienie, że wszystkie działania z zakresu informatyki śledczej są skoordynowane z obowiązkami prawnymi i regulacyjnymi, w tym w zakresie ochrony danych, prawa pracy oraz ograniczeń transferów międzynarodowych.

3.4 Wsparcie analiz poincydentalnych, ustalania przyczyny źródłowej oraz doskonalenia środków kontroli dzięki wysokiej jakości wynikom prac śledczych.

3.5 Integracja gotowości śledczej z Systemem Zarządzania Bezpieczeństwem Informacji (SZBI) w celu wsparcia audytów, zgłoszeń naruszeń oraz podejmowania decyzji przez kierownictwo.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO)

4.1.1 Jest właścicielem niniejszej polityki i zapewnia, że wszystkie działania z zakresu informatyki śledczej są prawnie defensywne, podlegają audytowi i są oparte na analizie ryzyka.

4.1.2 Autoryzuje eskalację do zewnętrznych podmiotów prawnych i dostawców usług informatyki śledczej.

4.2 Analitycy informatyki śledczej / personel obsługi incydentów

4.2.1 Odpowiadają za pozyskiwanie, zabezpieczanie i analizę techniczną materiału dowodowego.

4.2.2 Zapewniają prawidłowe rejestrowanie i utrzymanie łańcucha nadzoru.

4.2.3 Dokumentują wszystkie działania, ustalenia i konfiguracje narzędzi używanych podczas dochodzeń.

[... 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 poddawana przeglądowi co najmniej raz w roku i aktualizowana w razie potrzeby, aby odzwierciedlać:

9.1.1 zmiany w przepisach prawa, regulacjach lub orzecznictwie wpływające na procedury śledcze lub postępowanie z danymi

9.1.2 aktualizacje uznanych branżowo standardów lub narzędzi informatyki śledczej

9.1.3 wnioski z przeglądów poincydentalnych, sporów prawnych lub ustaleń audytowych

9.1.4 zmiany technologiczne dotyczące platform, urządzeń lub systemów objętych dochodzeniem

9.2 Właścicielem procesu przeglądu jest CISO, a proces ten musi obejmować konsultacje z:

9.2.1 działem prawnym i funkcją zgodności

9.2.2 Inspektorem Ochrony Danych (IOD)

9.2.3 zespołami operacji bezpieczeństwa i informatyki śledczej

9.2.4 funkcją audytu wewnętrznego / zgodności

9.3 Wszystkie zmiany muszą być:

9.3.1 objęte kontrolą wersji i przechowywane w repozytorium polityk

9.3.2 zakomunikowane zainteresowanym stronom, w tym zespołom śledczym i reagowania

9.3.3 powiązane z aktualizacją właściwych procedur operacyjnych i materiałów szkoleniowych

9.4 Przeglądy doraźne muszą być uruchamiane po każdym krytycznym incydencie związanym z niewłaściwym postępowaniem z materiałem dowodowym, naruszeniem łańcucha nadzoru lub problemami z dopuszczalnością prawną.

10. Powiązane polityki i odniesienia

10.1 Niniejsza polityka jest zgodna z następującymi politykami organizacyjnymi i jest przez nie wspierana:

10.1.1 P1 – P01 Polityka bezpieczeństwa informacji: ustanawia podstawowe wymagania dotyczące dochodzeń, kontroli materiału dowodowego oraz zgodności z właściwymi przepisami.

10.1.2 P5 – P05 Polityka zarządzania zmianą: zapewnia, że systemy objęte dochodzeniem nie są modyfikowane w trakcie aktywnych procesów śledczych.

10.1.3 P14 – Polityka retencji i utylizacji danych: określa zasady bezpiecznej utylizacji oraz okresy przechowywania materiału dowodowego i danych związanych ze sprawą.

10.1.4 P18 – Polityka zabezpieczeń kryptograficznych: określa wymagania dotyczące szyfrowania na potrzeby przechowywania i transferu danych wrażliwych lub mających charakter dowodowy.

10.1.5 P22 – Polityka logowania i monitorowania: zapewnia dostępność logów zdarzeń i telemetrii do celów pozyskiwania materiału dowodowego i korelacji śledczej.

10.1.6 P30 – Polityka reagowania na incydenty (P30): definiuje triage incydentów oraz ścieżki eskalacji uruchamiające procedury śledcze.

10.1.7 P33 – Polityka monitorowania audytu i zgodności: potwierdza przestrzeganie protokołów śledczych i wymagań dotyczących łańcucha nadzoru poprzez regularne audyty.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z międzynarodowymi standardami informatyki śledczej i obsługi incydentów, zapewniając integralność materiału dowodowego, prawnie defensywny charakter postępowania oraz zgodność w wielu jurysdykcjach.

11.2 ISO/IEC 27001

11.2.1 Klauzula 8.1 – wspiera kontrolę operacyjną gotowości śledczej i procedur dowodowych

11.3 ISO/IEC 27002

11.3.1 Załącznik A, środek kontroli 5.25 – Odpowiedzialności w zakresie zarządzania incydentami: wymaga zdefiniowanych ról dla obsługi incydentów bezpieczeństwa informacji i dochodzeń.

11.3.2 Załącznik A, środek kontroli 5.26 – Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji: wspiera gromadzenie artefaktów związanych ze zdarzeniami jako materiału dowodowego.

11.3.3 Załącznik A, środek kontroli 5.27 – Reagowanie na incydenty związane z bezpieczeństwem informacji: wymusza uporządkowaną remediację i dochodzenie oparte na materiale dowodowym.

11.3.4 Załącznik A, środek kontroli 8.27 – Bezpieczna architektura systemów i zasady inżynieryjne (jeżeli ma zastosowanie): odnosi się do ochrony systemów i narzędzi podczas dochodzeń.

11.4 ISO/IEC 27035:2016 (Części 1 i 3)

11.4.1 Określa zasady wykrywania incydentów, reagowania i gotowości śledczej, w tym planowania, łańcucha nadzoru oraz zarządzania materiałem dowodowym związanym z incydentem.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 do IR-9, AU-6, PL-2: definiuje uporządkowane wymagania dotyczące planowania, wykrywania, analizy, powstrzymania i reagowania na incydenty bezpieczeństwa. Wspiera gromadzenie materiału dowodowego i możliwość jego audytowania (AU-6) oraz zapewnia zgodność z planami bezpieczeństwa i prywatności systemów (PL-2) podczas dochodzeń śledczych.

11.6 NIST SP 800-86

11.6.1 Zawiera wytyczne dotyczące integracji procesów śledczych z szerszym cyklem życia reagowania na incydenty oraz zapewnienia gotowości śledczej.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Koncentruje się na dobrych praktykach pozyskiwania, zabezpieczania i analizowania dowodów z nośników cyfrowych oraz urządzeń mobilnych w sposób prawnie defensywny.

11.8 RODO (UE) 2016/679

11.8.1 Artykuł 5 – Zasady dotyczące przetwarzania danych osobowych: ma zastosowanie do materiału dowodowego zawierającego dane osobowe lub dane szczególnych kategorii, zapewniając minimalizację i ograniczenie celu.

11.8.2 Artykuły 33–34 – Zgłaszanie naruszeń ochrony danych osobowych: dane śledcze wspierają zgodność z obowiązkami zgłaszania naruszeń oraz procesami ujawniania informacji wymaganymi prawem.

11.9 Dyrektywa NIS2 (UE) 2022/2555

11.9.1 Artykuł 23 – obowiązki sprawozdawcze: dokumentacja śledcza i ustalenia wspierają terminowe i prawidłowe raportowanie incydentów do właściwych organów.

11.10 Rozporządzenie DORA (UE) 2022/2554

11.10.1 Artykuł 17 – Raportowanie incydentów ICT: wymaga szczegółowych zapisów dotyczących przyczyny źródłowej i materiału dowodowego dla poważnych incydentów związanych z ICT, w szczególności w sektorze finansowym.

11.11 COBIT 2019

11.11.1 DSS01.07 – Zarządzanie incydentami bezpieczeństwa: nakłada obowiązek dokumentowania incydentów i zachowania należytej staranności dochodzeniowej.

11.11.2 DSS05.04 – Zarządzanie dochodzeniami bezpieczeństwa: podkreśla znaczenie zabezpieczania dowodów cyfrowych oraz wsparcia działań dyscyplinarnych i prawnych.