					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P31S					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	Klauzule 6.1, 6.3, 8	Planowanie oparte na ryzyku, działania doskonalące oraz zabezpieczenia operacyjne zapewniające integralność materiału dowodowego
ISO/IEC 27002:2022	Środki kontrolne 5.24–5.27	Wytyczne dotyczące bezpiecznego postępowania, przeglądów po incydencie oraz doskonalenia opartego na materiale dowodowym
ISO/IEC 27035-3:2016	Klauzule 6.3, 6.4, 7	Zapewnia właściwe planowanie, zgodne z prawem gromadzenie oraz bezpieczne postępowanie z cyfrowym materiałem dowodowym wraz z dokumentacją łańcucha nadzoru
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Gotowość kryminalistyczna, ochrona logów audytowych oraz skuteczna integracja z reagowaniem na incydenty
RODO	Artykuły 33, 34	Dokumentowanie i identyfikowalność naruszeń ochrony danych osobowych
Dyrektywa NIS2	Artykuł 23	Identyfikowalne zgłaszanie incydentów i bezpieczne postępowanie z materiałem dowodowym
Rozporządzenie DORA	Artykuł 17(1), 17(2)	Zapewnia gromadzenie, przechowywanie i retencję materiału dowodowego dla incydentów związanych z ICT, poprawność kryminalistyczną oraz obsługę zapytań regulacyjnych
COBIT 2019	DSS05.06, DSS05.07	Wiarygodne rejestrowanie i uporządkowane postępowanie z materiałem dowodowym na potrzeby bezpiecznych dochodzeń podlegających kontroli audytowej

1. Cel

1.1. Niniejsza polityka określa zasady postępowania organizacji z cyfrowym materiałem dowodowym związanym z incydentami bezpieczeństwa, naruszeniami ochrony danych lub postępowaniami wewnętrznymi. Zapewnia, że materiał dowodowy jest gromadzony, przechowywany i zabezpieczany w sposób zgodny z wymaganiami prawnymi oraz zapewniający gotowość do audytu, wspierając zarówno decyzje wewnętrzne, jak i potencjalne działania zewnętrzne.

1.2. Polityka umożliwia małym organizacjom ochronę integralności logów, plików i obrazów systemów przy jednoczesnym wykazaniu należytej staranności zgodnie z ISO/IEC 27001, RODO oraz powiązanymi normami.

1.3. Polityka wspiera gotowość kryminalistyczną bez konieczności utrzymywania zaawansowanych zasobów technicznych lub pełnoetatowego zespołu IT poprzez określenie jasnych odpowiedzialności, procesów oraz wymagań dotyczących okresu przechowywania.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do:

2.1.1. wszystkich pracowników, dostawców usług IT oraz konsultantów zewnętrznych zaangażowanych w reagowanie na incydenty, dochodzenia lub analizę naruszeń

2.1.2. wszystkich systemów firmowych, w tym laptopów, urządzeń mobilnych, serwerów, kont poczty elektronicznej, platform SaaS oraz pamięci masowej w chmurze (np. Microsoft 365, Google Workspace)

2.1.3. każdego zdarzenia wymagającego materiału dowodowego na potrzeby wewnętrznych działań dyscyplinarnych, obrony prawnej, roszczeń ubezpieczeniowych lub kontaktów z organami regulacyjnymi

2.2. Obejmuje to zarówno zdarzenia rzeczywiste, jak i podejrzewane, związane z:

2.2.1. wyciekiem danych

2.2.2. zagrożeniami wewnętrznymi lub niewłaściwym użyciem

2.2.3. naruszeniami bezpieczeństwa (np. złośliwym oprogramowaniem, nieuprawnionym dostępem)

2.2.4. skargami klientów wymagającymi potwierdzenia w formie cyfrowej

2.2.5. zapytaniami organów regulacyjnych lub organów ścigania

3. Cele

3.1. Zapewnienie, że cały materiał dowodowy jest gromadzony i obsługiwany w sposób utrzymujący jego integralność, autentyczność oraz łańcuch nadzoru.

3.2. Zapobieganie przypadkowej modyfikacji, usunięciu lub niewłaściwej obsłudze logów, plików lub obrazów systemów, które mogą być potrzebne do dochodzeń.

3.3. Zapewnienie spójnego podejścia do zarządzania materiałem dowodowym, które podlega ścieżce audytu i spełnia wymagania prawne oraz regulacyjne (np. zgłoszenie naruszenia zgodnie z RODO, identyfikowalność wymagana przez NIS2).

3.4. Określenie jasnych ról i odpowiedzialności w celu zapewnienia szybkiego, bezpiecznego i zgodnego z prawem zabezpieczania materiału dowodowego podczas incydentów bezpieczeństwa.

3.5. Wspieranie gotowości kryminalistycznej na poziomie MŚP przy jednoczesnym ograniczeniu złożoności i unikaniu zakłóceń w bieżącej działalności operacyjnej.

4. Role i odpowiedzialności

4.1. Dyrektor Generalny (GM)

4.1.1. Zatwierdza wszystkie formalne dochodzenia wymagające gromadzenia materiału dowodowego.

4.1.2. Dokonuje przeglądu i zatwierdza raporty z incydentów obejmujące potencjalne działania prawne lub dyscyplinarne.

4.1.3. Decyduje, czy należy powiadomić zewnętrznego doradcę prawnego lub organy regulacyjne.

4.1.4. Zapewnia regularny przegląd i aktualizację polityki.

4.2. Dostawca usług IT / administrator systemu

4.2.1. Gromadzi i zabezpiecza cyfrowy materiał dowodowy zgodnie z bezpiecznymi procedurami.

4.2.2. Dokumentuje znaczniki czasu, szczegóły systemowe oraz wykonane czynności.

4.2.3. Zabezpiecza wszystkie zgromadzone materiały w chronionej lokalizacji.

4.2.4. Wspiera analizę kryminalistyczną, jeżeli jest wymagana.

[... 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 polityki

9.1.1. Niniejsza polityka musi być przeglądana co najmniej raz na 12 miesięcy przez Dyrektora Generalnego (GM) w celu potwierdzenia:

9.1.1.1. zgodności ze środkami kontrolnymi załącznika A do normy ISO/IEC 27001

9.1.1.2. dalszej adekwatności wobec aktualnych platform cyfrowych i usług IT

9.1.1.3. adekwatności procedur rejestrowania, okresu przechowywania materiału dowodowego oraz gotowości kryminalistycznej

9.2. Zdarzenia inicjujące zmianę polityki

9.2.1. Polityka musi być również przeglądana i aktualizowana po:

9.2.1.1. każdym istotnym incydencie wymagającym gromadzenia materiału dowodowego

9.2.1.2. nieudanym audycie lub żądaniu organu regulacyjnego, w ramach którego zakwestionowano integralność materiału dowodowego

9.2.1.3. wdrożeniu nowych narzędzi lub procedur reagowania na incydenty lub monitorowania systemów

9.2.1.4. zmianach prawnych (np. aktualizacji wytycznych RODO lub NIS2)

9.3. Zatwierdzanie zmian i dystrybucja

9.3.1. Wszystkie zmiany muszą zostać poddane przeglądowi i zatwierdzone przez GM

9.3.2. Zaktualizowana wersja musi zostać przekazana:

9.3.2.1. dostawcom usług IT i konsultantom zaangażowanym w dochodzenia

9.3.2.2. wszystkim osobom odpowiedzialnym za administrowanie systemami

9.3.3. Zaktualizowana kopia musi być przechowywana w archiwum polityk organizacji i udostępniana audytorom na żądanie

10. Powiązane polityki i zależności

10.1. Niniejsza polityka jest powiązana z następującymi politykami dostosowanymi do potrzeb MŚP:

10.1.1. P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: ustanawia uprawnienia w zakresie dochodzeń incydentów, decyzji dotyczących materiału dowodowego oraz eskalacji prawnej.

10.1.2. P4S – Polityka kontroli dostępu: zapewnia, że podczas dochodzeń dostęp do systemów wrażliwych i logów mają wyłącznie osoby upoważnione.

10.1.3. P22S – Polityka logowania i monitorowania: dostarcza dane źródłowe wykorzystywane jako materiał dowodowy oraz określa wymagania dotyczące okresu przechowywania, kontroli dostępu i rejestrowania.

10.1.4. P30S – Polityka reagowania na incydenty: inicjuje potrzebę gromadzenia materiału dowodowego i określa przebieg operacyjny prowadzący do zabezpieczenia materiału do celów kryminalistycznych.

10.1.5. P17S – Polityka ochrony danych i prywatności: zapewnia, że wszelkie dane osobowe gromadzone jako materiał dowodowy są przetwarzane zgodnie z prawem na podstawie RODO i powiązanych regulacji.

10.2. Polityki te działają łącznie, aby wspierać możliwość obrony z prawnego punktu widzenia, integralność dochodzeń oraz pełną gotowość do audytu zgodnie z ISO/IEC 27001:2022.

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 6.1 – Planowanie oparte na ryzyku obejmuje gotowość do reagowania oraz procedury dotyczące materiału dowodowego.

11.1.2. Klauzula 6.3 – Wspiera działania doskonalące oparte na materiale dowodowym z incydentów.

11.1.3. Klauzula 8.1 – Wymaga zabezpieczeń operacyjnych zapewniających integralność materiału dowodowego.

11.2. ISO/IEC 27002

11.2.1. Środki kontrolne 5.24–5.27 – Zawierają wytyczne dotyczące bezpiecznego postępowania, przeglądów po incydencie oraz doskonalenia opartego na materiale dowodowym.

11.3. ISO/IEC 27035-3

11.3.1. Klauzule 6.3, 6.4 oraz 7.3 zapewniają właściwe planowanie, zgodne z prawem gromadzenie oraz bezpieczne postępowanie z cyfrowym materiałem dowodowym podczas reagowania na incydenty, w tym jego zabezpieczenie i dokumentowanie łańcucha nadzoru.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 i AU-12 zapewniają gotowość kryminalistyczną, ochronę logów audytowych oraz skuteczną integrację gromadzenia materiału dowodowego z cyklem życia reagowania na incydenty

11.5. NIST SP 800-86

11.5.1. Określa dobre praktyki pozyskiwania, analizowania i ochrony cyfrowego materiału dowodowego podczas reagowania na incydenty.

11.6. RODO

11.6.1. Artykuły 33–34 – Wymagają dokumentowania i identyfikowalności incydentów oraz materiału dowodowego przy zgłaszaniu naruszeń ochrony danych osobowych.

11.7. Dyrektywa UE NIS2 (2022/2555)

11.7.1. Artykuł 23 – Wymaga identyfikowalnego zgłaszania incydentów oraz bezpiecznego postępowania z materiałem dowodowym przez podmioty kluczowe i ważne.

11.8. Rozporządzenie DORA

11.8.1. Artykuł 17(1) – Zapewnia, że materiał dowodowy związany z incydentami ICT jest gromadzony i przechowywany w sposób wspierający dochodzenia kryminalistyczne.

11.8.2. Artykuł 17(2) – Wymaga, aby podmioty finansowe przechowywały wszystkie istotne dane i logi związane ze zdarzeniami bezpieczeństwa informacji, zgodnie z zasadami poprawności kryminalistycznej oraz na potrzeby zapytań regulacyjnych.

11.9. COBIT 2019

11.9.1. DSS05.06 – Monitorowanie, wykrywanie i zgłaszanie incydentów: podkreśla znaczenie wiarygodnego rejestrowania na potrzeby wsparcia dochodzeń.

11.9.2. DSS05.07 – Badanie incydentów i podejmowanie działań: wymaga uporządkowanego postępowania z materiałem dowodowym w celu umożliwienia bezpiecznych dochodzeń podlegających kontroli audytowej.