					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P30S					Tytuł dokumentu: **Polityka reagowania na incydenty**							
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	zarządzanie incydentami, ciągłe doskonalenie, nadzór operacyjny
ISO/IEC 27002:2022	Środki kontrolne 5.24, 5.25	wykrywanie incydentów, gotowość, wyciąganie wniosków
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	obsługa incydentów, monitorowanie i raportowanie
RODO	Artykuł 33	wymagania dotyczące zgłaszania naruszeń
Dyrektywa NIS2	Artykuł 23	obowiązkowe zgłaszanie incydentów cyberbezpieczeństwa
Rozporządzenie DORA	Artykuł 17	zarządzanie incydentami ICT
COBIT 2019	DSS02, DSS04	zarządzanie zgłoszeniami usługowymi i incydentami oraz ciągłość działania

1. Cel

1.1. Niniejsza polityka określa sposób, w jaki organizacja wykrywa, zgłasza i obsługuje incydenty bezpieczeństwa informacji wpływające na jej systemy cyfrowe, dane lub usługi.

1.2. Polityka umożliwia organizacji ograniczenie szkód, ochronę danych klientów oraz spełnienie obowiązków regulacyjnych, takich jak wymóg zgłoszenia naruszenia w terminie 72 godzin zgodnie z RODO.

1.3. Polityka zapewnia jasny podział odpowiedzialności, zasady komunikacji oraz działania następcze po incydencie, również w małych organizacjach bez dedykowanego zespołu ds. bezpieczeństwa.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do:

2.1.1. wszystkich pracowników, kontrahentów i zewnętrznych dostawców usług IT

2.1.2. wszystkich systemów i usług zarządzanych przez organizację, w tym stron internetowych, platform chmurowych, urządzeń mobilnych, laptopów i kont poczty elektronicznej

2.1.3. wszystkich rodzajów incydentów, w tym:

2.1.3.1. nieuprawnionego dostępu do danych lub systemów

2.1.3.2. infekcji złośliwym oprogramowaniem lub ransomware

2.1.3.3. prób phishingu lub socjotechniki

2.1.3.4. niedostępności systemów spowodowanej cyberatakiem lub niewłaściwym użyciem

2.1.3.5. przypadkowego ujawnienia lub usunięcia danych wrażliwych

2.1.3.6. utraty lub kradzieży urządzeń służbowych lub nośników danych

3. Cele

3.1. Ustanowić jasny proces identyfikacji i eskalacji incydentów bezpieczeństwa.

3.2. Zapewnić, że incydenty są zgłaszane, rejestrowane i obsługiwane w określonych ramach czasowych.

3.3. Umożliwić szybkie ograniczenie skutków, odtworzenie danych i przywrócenie usług.

3.4. Zapewnić, że strony, których to dotyczy (np. klienci, organy regulacyjne), są powiadamiane, gdy wymagają tego przepisy prawa.

3.5. Zapobiegać ponownemu wystąpieniu incydentów poprzez analizę przyczyny źródłowej, działania korygujące oraz doskonalenie polityki.

3.6. Umożliwić MŚP spełnienie wymagań certyfikacyjnych ISO/IEC 27001 oraz wykazanie rozliczalności podczas audytów.

4. Role i odpowiedzialności

4.1. Dyrektor Generalny (GM)

4.1.1. Jest właścicielem niniejszej polityki i odpowiada za jej wdrożenie.

4.1.2. Nadzoruje działania związane z reagowaniem na incydenty oraz zatwierdza powiadomienia kierowane do organów regulacyjnych lub klientów.

4.1.3. Przegląda raporty po incydencie i zapewnia aktualizację polityki, jeżeli jest to wymagane.

4.1.4. Może delegować obowiązki koordynacyjne, zachowując rozliczalność.

4.2. Dostawca wsparcia IT / administrator systemów (wewnętrzny lub zewnętrzny)

4.2.1. Wykrywa i analizuje potencjalne incydenty bezpieczeństwa.

4.2.2. Wdraża działania związane z ograniczeniem skutków i odtwarzaniem (np. wyłączenie dostępu, odtworzenie kopii zapasowych).

4.2.3. Powiadamia GM o wszystkich potwierdzonych lub podejrzewanych incydentach w ciągu 1 godziny od ich wykrycia.

4.2.4. Utrzymuje rejestr incydentów zawierający znaczniki czasu, ocenę wpływu oraz podjęte działania.

[... 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. Planowany przegląd

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

9.1.1.1. zgodności ze środkami kontrolnymi ISO/IEC 27001:2022

9.1.1.2. adekwatności wobec nowych zagrożeń, ryzyk i incydentów

9.1.1.3. dalszej zgodności z obowiązkami prawnymi i umownymi (np. RODO, DORA)

9.2. Zdarzenia uruchamiające przegląd

9.2.1. Polityka musi być również przeglądana i aktualizowana po:

9.2.1.1. każdym incydencie o wysokiej wadze lub powiadomieniu regulacyjnym

9.2.1.2. wdrożeniu nowej infrastruktury IT lub zmian systemowych

9.2.1.3. zmianach wymagań prawnych dotyczących naruszeń bezpieczeństwa

9.3. Dokumentowanie przeglądu i dystrybucja

9.3.1. Wszystkie przeglądy i zmiany muszą być dokumentowane w dzienniku zmian polityki

9.3.2. Zaktualizowane wersje muszą zostać przekazane wszystkim pracownikom, dostawcom i dostawcom wsparcia IT zaangażowanym w bezpieczeństwo lub operacje systemowe

9.3.3. Dowody świadomości personelu (np. notatki ze spotkań lub potwierdzenia e-mail) muszą być przechowywane w celu zapewnienia gotowości do audytu

10. Powiązane polityki i zależności

10.1. Niniejszą politykę należy stosować łącznie z następującymi politykami SME:

10.1.1. P1S – Polityka bezpieczeństwa informacji: określa ogólne oczekiwania dotyczące utrzymania poufności, integralności i dostępności (CIA) w trakcie działalności operacyjnej, w tym obsługi incydentów.

10.1.2. P2S – Polityka ról i odpowiedzialności w ramach ładu organizacyjnego: ustanawia strukturę uprawnień i rozliczalności dla wykrywania, zgłaszania i eskalacji incydentów.

10.1.3. P4S – Polityka kontroli dostępu: umożliwia natychmiastowe cofnięcie dostępu w ramach działań reagowania na incydenty.

10.1.4. P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia, że wszyscy pracownicy potrafią skutecznie identyfikować i zgłaszać incydenty bezpieczeństwa.

10.1.5. P17S – Polityka ochrony danych i prywatności: określa procedury prawne zgłaszania naruszeń zgodnie z RODO i wspiera zgodność regulacyjną podczas incydentów.

10.1.6. P22S – Polityka logowania i monitorowania: zapewnia niezbędne narzędzia oraz widoczność potrzebne do wykrywania, analizowania i audytu zdarzeń bezpieczeństwa informacji.

10.1.7. P31S – Polityka gromadzenia dowodów i informatyki śledczej: wspiera postępowanie wyjaśniające oraz możliwość obrony prawnej działań związanych z incydentem poprzez właściwe postępowanie z materiałem dowodowym.

10.2. Polityki te łącznie ustanawiają operacyjne ramy MŚP dla wykrywania incydentów bezpieczeństwa informacji, reagowania na nie oraz odtwarzania po nich.

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 6.1 – wymaga planowania postępowania z ryzykiem, w tym przygotowania do obsługi incydentów.

11.1.2. Klauzula 6.3 – wspiera ciągłe doskonalenie poprzez wyciąganie wniosków ze zdarzeń związanych z bezpieczeństwem informacji.

11.1.3. Klauzula 8.1 – podkreśla znaczenie nadzoru operacyjnego dla zarządzania incydentami i zakłóceniami.

11.2. ISO/IEC 27002

11.2.1. Środek kontrolny 5.24 – wymaga ustrukturyzowanego podejścia do zgłaszania, oceny i reagowania na incydenty bezpieczeństwa informacji.

11.2.2. Środek kontrolny 5.25 – koncentruje się na wyciąganiu wniosków z incydentów w celu poprawy przyszłej gotowości i odporności systemów.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – definiuje procedury obsługi incydentów, w tym ograniczenie skutków i odtwarzanie.

11.3.2. IR-5 – ustanawia wymagania dotyczące monitorowania i analizy incydentów.

11.3.3. IR-6 – nakłada wymóg stosowania wewnętrznych i zewnętrznych zasad zgłaszania incydentów.

11.4. RODO

11.4.1. Artykuł 33 – wymaga zgłaszania naruszeń ochrony danych osobowych organom nadzorczym w ciągu 72 godzin wraz z informacjami o zakresie i działaniach ograniczających skutki.

11.5. Dyrektywa NIS2 (2022/2555)

11.5.1. Artykuł 23 – wymaga od podmiotów kluczowych i ważnych zgłaszania istotnych incydentów właściwym organom z wykorzystaniem ustandaryzowanych formatów raportowania.

11.6. Rozporządzenie DORA (2022/2554)

11.6.1. Artykuł 17 – wymaga od podmiotów finansowych klasyfikowania, zgłaszania i śledzenia incydentów oraz zakłóceń związanych z ICT.

11.7. COBIT 2019

11.7.1. DSS02 – Zarządzanie zgłoszeniami usługowymi i incydentami: wskazuje sposób skutecznej obsługi incydentów operacyjnych i bezpieczeństwa zgodnie z celami ładu organizacyjnego.

11.7.2. DSS04 – Zarządzanie ciągłością: łączy reagowanie na incydenty z szerszymi strategiami ciągłości działania i odtwarzania.