					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P12					Tytuł dokumentu: **Polityka zarządzania aktywami**							
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**

1. Cel

1.1 Niniejsza polityka określa obowiązkowe wymagania organizacyjne dotyczące identyfikacji, klasyfikacji, zarządzania oraz ochrony aktywów informacyjnych w całym ich cyklu życia. Wspiera nadzór nad aktywami sprzętowymi, programowymi, danymi, aktywami chmurowymi oraz niematerialnymi aktywami informacyjnymi w całej organizacji, w tym w środowiskach mobilnych, zdalnych oraz zarządzanych przez strony trzecie.

1.2 Celem niniejszej polityki jest zapewnienie pełnej widoczności zasobów informacyjnych organizacji, tak aby umożliwić stosowanie skutecznych zabezpieczeń, przypisanie właścicieli, zapewnienie zgodności oraz odpowiednie wycofanie z eksploatacji lub utylizację.

1.3 Polityka jest zgodna z ISO/IEC 27001:2022, Załącznik A.5.9, poprzez obowiązek utrzymywania scentralizowanego inwentarza informacji i powiązanych aktywów. Zapewnia rozliczalność przez przypisanie każdego aktywa do właściciela oraz stosowanie ochrony wynikającej z klasyfikacji, odpowiednio do wrażliwości biznesowej i wymagań regulacyjnych.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich pracowników, współpracowników, dostawców zewnętrznych oraz usługodawców, którzy zarządzają aktywami informacyjnymi będącymi własnością organizacji lub pozostającymi pod jej kontrolą, korzystają z nich, uzyskują do nich dostęp, przechowują je lub przetwarzają.

2.2 Zakres obejmuje wszystkie kategorie aktywów, w tym:

2.2.1 Aktywa fizyczne: laptopy, komputery stacjonarne, urządzenia mobilne, nośniki wymienne, drukarki, urządzenia sieciowe

2.2.2 Aktywa cyfrowe: oprogramowanie, aplikacje, obrazy systemów, bazy danych, dane kopii zapasowych, klucze szyfrujące

2.2.3 Aktywa informacyjne: dane ustrukturyzowane i nieustrukturyzowane, raporty, wiadomości e-mail, własność intelektualna

2.2.4 Aktywa chmurowe i wirtualne: środowiska IaaS, SaaS, PaaS, maszyny wirtualne, kontenery

2.2.5 Aktywa logiczne: nazwy domen, licencje, konta użytkowników, konfiguracje bazowe

2.3 Polityka reguluje również aktywa wykorzystywane w środowiskach pracy zdalnej, hybrydowej lub outsourcingowej, zapewniając ich ochronę i widoczność nawet wtedy, gdy aktywa nie znajdują się fizycznie na terenie organizacji.

3. Cele

3.1 Utrzymywanie kompletnego, dokładnego i aktualnego inwentarza wszystkich aktywów informacyjnych organizacji wraz z określonym właścicielem, klasyfikacją i lokalizacją.

3.2 Przypisanie właścicieli aktywów odpowiedzialnych za klasyfikację, postępowanie z aktywami i ochronę aktywów pozostających pod ich kontrolą, zgodnie z politykami zarządzania danymi i bezpieczeństwa.

3.3 Stosowanie odpowiedniej klasyfikacji i oznakowania do wszystkich aktywów na podstawie ich wrażliwości, krytyczności oraz uwarunkowań regulacyjnych.

3.4 Ochrona aktywów zgodnie z ich klasyfikacją i powiązaną ekspozycją na ryzyko, w tym w zakresie przechowywania, dostępu, transmisji i utylizacji.

3.5 Egzekwowanie procedur zwrotu aktywów i bezpiecznej utylizacji podczas zakończenia współpracy z pracownikiem, zakończenia umowy lub zakończenia cyklu życia aktywa.

3.6 Wspieranie zgodności regulacyjnej z takimi ramami jak ISO/IEC 27001, RODO, NIS2, DORA i COBIT 2019 poprzez ustrukturyzowane zarządzanie aktywami oraz zapewnienie ścieżki audytowej.

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze

4.1.1 Zatwierdza Politykę zarządzania aktywami i zapewnia przydzielenie zasobów niezbędnych do jej pełnego wdrożenia.

4.1.2 Ponosi ostateczną odpowiedzialność za zapewnienie, że aktywa organizacji są chronione i zarządzane zgodnie z obowiązkami regulacyjnymi oraz umownymi.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO)

4.2.1 Jest właścicielem Polityki zarządzania aktywami i zapewnia jej integrację z szerszym systemem zarządzania bezpieczeństwem informacji (SZBI) organizacji.

4.2.2 Dokonuje przeglądu odstępstw i odchyleń od niniejszej polityki oraz wymaga stosowania strategii ograniczania ryzyka opartych na analizie ryzyka.

4.2.3 Nadzoruje okresowe audyty klasyfikacji aktywów, integralności inwentarza oraz zgodności zarządzania cyklem życia aktywów.

[... 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 podlegać przeglądowi co najmniej raz w roku lub w odpowiedzi na:

9.1.1 Zmiany obowiązków prawnych lub regulacyjnych wpływających na klasyfikację aktywów lub wymagania dotyczące inwentarza

9.1.2 Wprowadzenie nowych kategorii aktywów lub platform zarządzania (np. natywnych chmurowo systemów CMDB)

9.1.3 Ustalenia audytu wewnętrznego lub incydenty bezpieczeństwa związane z niewłaściwym zarządzaniem aktywami

9.1.4 Restrukturyzację organizacyjną wpływającą na własność aktywów lub zabezpieczenia cyklu życia

9.2 Proces przeglądu musi zostać zainicjowany przez Menedżera ds. aktywów IT i skoordynowany z CISO, funkcją zakupów, działem prawnym i zgodności oraz właściwymi kierownikami działów.

9.3 Przeglądy doraźne mogą być również uruchamiane przez:

9.3.1 Nabycie lub zbycie jednostek biznesowych

9.3.2 Zmiany dostawców wpływające na aktywa zarządzane przez strony trzecie

9.3.3 Odświeżenia technologiczne obejmujące masowe wycofanie z eksploatacji lub przydzielanie zasobów

9.4 Wszystkie zmiany niniejszej polityki muszą:

9.4.1 Podlegać kontroli wersji i być przechowywane w repozytorium SZBI

9.4.2 Zostać zatwierdzone przez kierownictwo wykonawcze

9.4.3 Zawierać podsumowanie zmian oraz uzasadnienie

9.4.4 Zostać zakomunikowane wszystkim zainteresowanym stronom, wraz ze zaktualizowanymi procedurami lub szkoleniami systemowymi, jeżeli ma to zastosowanie

10. Powiązane polityki i zależności

10.1 Niniejsza polityka funkcjonuje łącznie z następującymi politykami powiązanymi i wspiera stosowanie ich postanowień:

10.1.1 P4 - Polityka kontroli dostępu: Zapewnia zgodność widoczności aktywów z uprawnieniami dostępu i mechanizmami kontroli w systemach oraz środowiskach danych.

10.1.2 P7 - Polityka wdrażania i zakończenia współpracy: Reguluje terminowe nadawanie oraz zwrot aktywów fizycznych i logicznych podczas zmian kadrowych.

10.1.3 P13 - Polityka klasyfikacji danych i oznakowania: Ustanawia obowiązkowe zasady klasyfikacji aktywów, które określają procedury oznakowania, postępowania i utylizacji.

10.1.4 P14 - Polityka retencji danych i utylizacji: Określa terminy oraz metody bezpiecznej utylizacji cyfrowych i fizycznych aktywów zawierających informacje.

10.1.5 P22 - Polityka rejestrowania i monitorowania: Umożliwia zapewnienie ścieżki audytowej dostępu do aktywów i ich wykorzystania poprzez rejestrowanie systemowe, widoczność punktów końcowych i analitykę behawioralną.

10.1.6 P30 - Polityka reagowania na incydenty: Wspiera szybkie powstrzymanie i dochodzenie w przypadku naruszeń związanych z aktywami, takich jak utracone laptopy lub nieewidencjonowane nośniki pamięci.

10.2 Polityki te tworzą spójną strukturę ładu zarządczego zapewniającą, że aktywa są bezpiecznie zarządzane, prawidłowo ewidencjonowane i odpowiednio obsługiwane w całym cyklu życia.

11. Normy odniesienia i ramy

11.1 Niniejsza polityka jest zgodna z uznanymi międzynarodowo normami bezpieczeństwa informacji i ramami regulacyjnymi, które wymagają skutecznego zarządzania aktywami w całym cyklu życia.

11.2 ISO/IEC 27001:

11.2.1 Klauzula 8.1 - Wymaga od organizacji planowania, wdrażania i nadzorowania procesów niezbędnych do spełnienia wymagań bezpieczeństwa informacji, w tym dotyczących zarządzania cyklem życia aktywów.

11.3 ISO/IEC 27002:2022 - Środki kontrolne 5.9 do 5.11

11.3.1 Klauzula 5.9 - Inwentarz informacji i innych powiązanych aktywów: Wymaga aktualnego i kompletnego inwentarza wszystkich aktywów istotnych dla przetwarzania informacji.

11.3.2 Klauzula 5.10 - Dopuszczalne użytkowanie informacji i aktywów: Wspierane przez zasady użytkowania, własność oraz procesy zwrotu.

11.3.3 Klauzula 5.11 - Zwrot aktywów: Wdrożone poprzez formalne procedury przekazania i wycofania z eksploatacji.

11.3.4 Środki kontrolne te ustanawiają ustrukturyzowane wymagania dotyczące identyfikacji, oznakowania, utrzymywania i śledzenia aktywów organizacji, wraz z odpowiednimi odpowiedzialnościami właścicieli i opiekunów w całym cyklu życia.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Inwentarz komponentów systemu: Odzwierciedlone poprzez scentralizowane zarządzanie aktywami, widoczność w czasie rzeczywistym oraz powiązanie z konfiguracjami operacyjnymi.

11.4.2 RA-3 - Ocena ryzyka: Inwentarze aktywów stanowią podstawowy element modelowania zagrożeń i oceny ryzyka.

11.4.3 MP-6 - Oczyszczanie nośników: Egzekwowane poprzez bezpieczne metody utylizacji określone w zabezpieczeniach cyklu życia aktywów oraz Polityce utylizacji danych.

11.5 RODO (2016/679):

11.5.1 Artykuł 30 - Rejestry czynności przetwarzania: Wymaga od organizacji dokumentowania systemów, urządzeń i repozytoriów, które przechowują lub przetwarzają dane osobowe.

11.5.2 Artykuł 32 - Bezpieczeństwo przetwarzania: Jest zgodny z oceną ryzyka opartą na aktywach oraz środkami bezpieczeństwa dostosowanymi do sklasyfikowanych aktywów i infrastruktury krytycznej.

11.6 Dyrektywa NIS2 (2022/2555):

11.6.1 Artykuł 21(2)(a, b): Nakłada obowiązek zapewnienia widoczności aktywów i prowadzenia ich inwentarza jako podstawy analizy ryzyka, ochrony i reagowania na incydenty cyberbezpieczeństwa.

11.6.2 Artykuł 21(3): Podkreśla konieczność stosowania ustrukturyzowanego nadzoru nad aktywami jako elementu kultury bezpieczeństwa organizacji.

11.7 Rozporządzenie DORA (2022/2554):

11.7.1 Artykuł 5 - Ład ICT i kontrola wewnętrzna: Wymaga od podmiotów finansowych nadzorowania aktywów ICT z zapewnieniem jasnych wymagań dotyczących inwentarza, własności i ochrony.

11.7.2 Artykuł 9 - Ramy zarządzania ryzykiem ICT: Stanowi, że procesy zarządzania aktywami muszą wspierać ograniczanie zagrożeń, planowanie ciągłości działania oraz odporność usług.

11.8 COBIT 2019:

11.8.1 BAI09 - Zarządzanie aktywami: Bezpośrednio zgodne z ustrukturyzowaną identyfikacją, klasyfikacją, wykorzystaniem i utylizacją aktywów organizacji.

11.8.2 DSS01 - Zarządzane operacje: Wspiera wdrożenie zabezpieczeń zapewniających ochronę aktywów i ciągły nadzór operacyjny.

11.8.3 MEA03 - Monitorowanie, ocena i ocena zgodności: Zapewnia regularne audytowanie zabezpieczeń zarządzania aktywami oraz ich skuteczności w zapewnianiu zgodności regulacyjnej.