					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P12S					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**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8	Wymagania dotyczące zarządzania aktywami
ISO/IEC 27002:2022	Środek kontrolny 5	Środki kontroli dotyczące zarządzania aktywami
NIST SP 800-53 Rev. 5	CM-8	Inwentarz komponentów systemu
Dyrektywa NIS2	Artykuł 21(2)(a)	Ewidencjonowanie aktywów na potrzeby ochrony systemów sieci i informacji
Rozporządzenie DORA	Artykuł 5(8)	Wymagania dotyczące inwentarza aktywów ICT
COBIT 2019	BAI	Zarządzanie cyklem życia aktywów IT
RODO	Artykuł 30	Rejestr czynności przetwarzania

1. Cel

1.1 Niniejsza polityka określa sposób, w jaki organizacja identyfikuje, ewidencjonuje, chroni i wycofuje z użytkowania swoje aktywa informacyjne, w tym zarówno składniki fizyczne, jak i cyfrowe.

1.2 Celem jest ograniczenie ryzyka operacyjnego i ryzyka bezpieczeństwa poprzez zapewnienie widoczności, rozliczalności oraz bezpiecznego postępowania ze wszystkimi aktywami biznesowymi w całym ich cyklu życia.

1.3 Wiarygodny inwentarz aktywów wspiera zgodność z wymaganiami regulacyjnymi, reagowanie na incydenty, planowanie ciągłości działania oraz zarządzanie ryzykiem.

1.4 Niniejsza polityka wspiera również certyfikację zgodnie z ISO/IEC 27001 oraz wykazywanie zgodności z obowiązkami prawnymi, finansowymi i z zakresu cyberbezpieczeństwa wynikającymi z takich ram jak RODO, NIS2 i DORA.

1.5 W przypadku małych i średnich przedsiębiorstw (MŚP) proste, ale systematyczne podejście do zarządzania aktywami jest niezbędne, aby unikać niezarządzanych urządzeń, wycieków danych lub niezgodności stwierdzanych podczas audytu, zwłaszcza przy ograniczonych zasobach kadrowych w obszarze technicznym.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich aktywów będących własnością organizacji, leasingowanych lub w inny sposób przez nią zarządzanych, w tym wykorzystywanych w:

2.1.1 pracy biurowej

2.1.2 pracy zdalnej lub hybrydowej

2.1.3 działaniach terenowych lub mobilnych

2.1.4 środowiskach chmurowych i usługach outsourcingowych

2.2 Zakres obejmuje między innymi następujące typy aktywów:

2.2.1 Sprzęt: laptopy, komputery stacjonarne, monitory, telefony, tablety, nośniki USB, routery, drukarki, nośniki kopii zapasowych

2.2.2 Oprogramowanie: zainstalowane aplikacje, usługi SaaS, systemy operacyjne, oprogramowanie antywirusowe, licencje

2.2.3 Aktywa informacyjne: repozytoria danych biznesowych, arkusze kalkulacyjne, rejestry klientów, kod źródłowy

2.2.4 Tożsamości cyfrowe i usługi: nazwy domen, certyfikaty cyfrowe, klucze API, konta poczty elektronicznej, dostępy do chmury

2.2.5 Urządzenia dostępowe: klucze, karty inteligentne, breloki dostępowe, tokeny biometryczne

2.3 Niniejsza polityka dotyczy wszystkich pracowników, współpracowników oraz dostawców usług zewnętrznych, którzy korzystają z aktywów organizacji.

2.4 Polityka reguluje również zarówno aktywa krótkoterminowe (np. laptopy przypisane do konkretnego projektu), jak i długoterminowe, a także aktywa współdzielone używane przez wiele osób z personelu.

3. Cele

3.1 Ustanowić i utrzymywać kompletny oraz dokładny inwentarz aktywów obejmujący wszystkie istotne aktywa, aktualizowany na bieżąco.

3.2 Zapewnić, aby każde aktywo miało wyznaczonego właściciela odpowiedzialnego za jego użytkowanie, przechowywanie i zwrot.

3.3 Klasyfikować aktywa na podstawie wrażliwości, wpływu biznesowego lub znaczenia regulacyjnego, tak aby możliwe było stosowanie zróżnicowanych poziomów ochrony.

3.4 Określić jednoznaczne procedury wydawania aktywów, ich ponownego przypisania, utrzymania, zgłaszania utraty oraz wycofywania z użytkowania.

3.5 Zapewnić bezpieczne postępowanie z aktywami przez cały ich cykl życia oraz ochronę informacji, które przechowują, albo ich bezpieczne usunięcie przy utylizacji.

3.6 Ograniczyć prawdopodobieństwo incydentów bezpieczeństwa spowodowanych przez nieewidencjonowane, niezwrócone lub niewłaściwie wykorzystywane zasoby organizacji.

3.7 Wspierać zgodność z właściwymi przepisami prawa (np. zasadą rozliczalności wynikającą z RODO) oraz normami certyfikacyjnymi w obszarze cyberbezpieczeństwa.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Odpowiada za niniejszą politykę oraz za zapewnienie, że praktyki zarządzania aktywami są wdrożone i przestrzegane w całej organizacji.

4.1.2 Dokonuje przeglądu i zatwierdza aktualizacje inwentarza aktywów oraz zatwierdza wycofanie z eksploatacji lub przekazanie aktywów, jeżeli jest to wymagane.

4.1.3 Musi być informowany o każdej istotnej utracie, kradzieży lub niewłaściwym użyciu aktywów.

4.2 Lider IT lub wyznaczony opiekun aktywów

4.2.1 Utrzymuje inwentarz aktywów (np. w arkuszu kalkulacyjnym, systemie zgłoszeniowym lub uproszczonym narzędziu do ewidencji aktywów).

4.2.2 Przypisuje właścicieli aktywów i ewidencjonuje zmiany statusu (np. nowe, w użyciu, w naprawie, wycofane).

4.2.3 Weryfikuje, że wszystkie wydane aktywa są udokumentowane i powiązane z konkretną osobą lub jednostką organizacyjną.

4.2.4 Zapewnia stosowanie i przestrzeganie etykiet klasyfikacyjnych (np. Wewnętrzne, Poufne).

4.2.5 Koordynuje odzyskiwanie aktywów, ich bezpieczne czyszczenie oraz dezaktywację w ramach offboardingu lub wycofywania z użytkowania.

4.2.6 Zgłasza wszelkie nierozwiązane rozbieżności dotyczące aktywów do GM.

[... 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 oraz każdorazowo, gdy:

9.1.1 wprowadzane są nowe typy technologii lub aktywów

9.1.2 zmieniają się procedury ewidencjonowania aktywów (np. poprzez wdrożenie nowych narzędzi lub platform)

9.1.3 nowe obowiązki regulacyjne wpływają na identyfikowalność aktywów lub ich utylizację

9.1.4 incydent lub audyt wskaże lukę w aktualnych praktykach zarządzania aktywami

9.2 W przeglądach muszą uczestniczyć GM i Lider IT, a ich zakres musi obejmować aktualizację procedur postępowania z aktywami, szablonów inwentarza oraz wytycznych klasyfikacyjnych.

9.3 Wszystkie aktualizacje muszą być dokumentowane i komunikowane odpowiednim członkom personelu. Należy prowadzić rejestr zmian objęty kontrolą wersji.

10. Powiązane polityki i zależności

10.1 P2S – Polityka ról i odpowiedzialności w ramach ładu organizacyjnego: określa rozliczalność za właścicielstwo polityk i operacje IT.

10.2 P4S – Polityka kontroli dostępu: wiąże użytkowanie aktywów (np. laptopów, urządzeń mobilnych) z uprawnieniami dostępowymi użytkowników i zarządzaniem tożsamością.

10.3 P7S – Polityka wdrażania i zakończenia współpracy: zapewnia uwzględnienie wydawania i odzyskiwania aktywów w procesach cyklu życia personelu.

10.4 P13S – Polityka klasyfikacji i oznaczania danych: określa zasady ustalania, czy aktywo powinno być sklasyfikowane jako Wewnętrzne czy Poufne.

10.5 P30S – Polityka reagowania na incydenty: określa procedury reagowania, jeśli zdarzenie związane z aktywem prowadzi do naruszenia bezpieczeństwa lub prywatności.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1: wymaga stosowania zabezpieczeń operacyjnych w celu zarządzania aktywami i ich ochrony przez cały okres użytkowania.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 5.9: określa sposób identyfikacji aktywów, przypisywania właściciela, klasyfikacji oraz bezpiecznego zarządzania aktywami.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-8: wymaga, aby organizacje opracowały i utrzymywały inwentarz komponentów systemu, w tym sprzętu, oprogramowania i aktywów wirtualnych.

11.4 RODO

11.4.1 Artykuł 30: wymaga dokumentowania czynności przetwarzania danych, co zależy od wiedzy o tym, gdzie dane są przechowywane i na jakich aktywach.

11.5 Dyrektywa NIS2

11.5.1 Artykuł 21(2)(a): wymaga stosowania środków technicznych i organizacyjnych, w tym ewidencjonowania aktywów, w celu ochrony systemów sieci i informacji.

11.6 Rozporządzenie DORA

11.6.1 Artykuł 5(8): podmioty finansowe muszą utrzymywać szczegółowe inwentarze aktywów ICT jako element zarządzania ryzykiem ICT.

11.7 COBIT 2019

11.7.1 BAI09: określa, że aktywa IT muszą być zarządzane w całym ich cyklu życia — od pozyskania do wycofania z użytkowania — z jasno przypisanym właścicielem i odpowiednimi środkami kontroli.