					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P12					Titlul documentului: **Politica de management al activelor**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

1. Scop

1.1 Această politică definește cerințele organizaționale obligatorii pentru identificarea, clasificarea, gestionarea și protejarea activelor informaționale pe întreg ciclul lor de viață. Aceasta susține guvernanța la nivelul întregii organizații a activelor hardware, software, de date, cloud și a activelor informaționale necorporale, inclusiv în medii mobile, la distanță și administrate de terți.

1.2 Scopul acestei politici este de a asigura vizibilitate completă asupra peisajului activelor informaționale ale organizației, permițând implementarea eficace a controalelor de securitate, atribuirea responsabilității de proprietate, alinierea la cerințele de conformitate și dezafectarea sau eliminarea responsabilă.

1.3 Politica este aliniată cu controlul A.5.9 din ISO/IEC 27001:2022 prin impunerea menținerii unui inventar centralizat al informațiilor și al activelor asociate. Aceasta asigură responsabilizarea prin asocierea fiecărui activ cu un proprietar și prin aplicarea unei protecții determinate de clasificare, în funcție de sensibilitatea pentru activitățile organizației și de cerințele de reglementare.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor angajaților, contractanților, furnizorilor terți și prestatorilor de servicii care gestionează, utilizează, accesează, stochează sau prelucrează active informaționale deținute sau controlate de organizație.

2.2 Domeniul de aplicare include toate categoriile de active, cum ar fi:

2.2.1 Active fizice: laptopuri, desktopuri, dispozitive mobile, medii amovibile, imprimante, echipamente de rețea

2.2.2 Active digitale: software, aplicații, imagini de sistem, baze de date, date de backup, chei criptografice

2.2.3 Active informaționale: date structurate și nestructurate, rapoarte, e-mailuri, proprietate intelectuală

2.2.4 Active cloud și virtuale: medii IaaS, SaaS, PaaS, mașini virtuale, containere

2.2.5 Active logice: nume de domeniu, licențe, conturi de utilizator, configurații de referință

2.3 Politica reglementează, de asemenea, activele utilizate în medii de telemuncă, hibride sau externalizate, asigurând protecție și vizibilitate chiar și atunci când activele nu sunt localizate fizic în sediile organizației.

3. Obiective

3.1 Menținerea unui inventar complet, exact și actualizat al tuturor activelor informaționale ale organizației, cu atribute definite privind proprietatea, clasificarea și localizarea.

3.2 Desemnarea proprietarilor de active responsabili pentru clasificarea, gestionarea și protecția activelor aflate sub controlul lor, în conformitate cu politicile de guvernanță a datelor și de securitate.

3.3 Aplicarea unei clasificări și etichetări adecvate tuturor activelor, pe baza sensibilității, criticității și cerințelor de reglementare.

3.4 Protejarea activelor în funcție de clasificarea lor și de expunerea la risc asociată, inclusiv în ceea ce privește stocarea, accesul, transmiterea și eliminarea.

3.5 Aplicarea procedurilor de returnare a activelor și de eliminare securizată la încetarea raporturilor de muncă, la încetarea contractelor sau la finalul ciclului de viață al activelor.

3.6 Susținerea conformității cu cerințele aplicabile din cadre precum ISO/IEC 27001, GDPR, NIS2, DORA și COBIT 2019, printr-un management structurat al activelor și trasabilitate pentru audit.

4. Roluri și responsabilități

4.1 Conducerea executivă

4.1.1 Aprobă Politica de management al activelor și se asigură că sunt alocate resursele necesare pentru implementarea integrală a acesteia.

4.1.2 Deține responsabilitatea finală pentru a se asigura că activele organizației sunt protejate și gestionate în conformitate cu obligațiile de reglementare și contractuale.

4.2 Directorul de securitate a informațiilor (CISO)

4.2.1 Deține Politica de management al activelor și asigură integrarea acesteia în Sistemul de management al securității informațiilor (SMSI) al organizației.

4.2.2 Revizuiește excepțiile și abaterile de la această politică și impune măsuri de atenuare bazate pe risc.

4.2.3 Asigură supravegherea auditurilor periodice privind clasificarea activelor, integritatea inventarului și respectarea cerințelor aferente ciclului de viață al activelor.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Cerințe de revizuire și actualizare

9.1 Această politică trebuie revizuită cel puțin anual sau ca răspuns la:

9.1.1 modificări ale obligațiilor legale sau de reglementare care afectează clasificarea activelor sau cerințele de inventariere

9.1.2 introducerea de noi categorii de active sau platforme de management (de exemplu, CMDB-uri native cloud)

9.1.3 constatări ale auditului intern sau incidente de securitate care implică gestionarea defectuoasă a activelor

9.1.4 reorganizări interne care afectează proprietatea sau controalele ciclului de viață

9.2 Procesul de revizuire trebuie inițiat de Managerul de active IT și coordonat cu CISO, Achiziții, Juridic și șefii de departament afectați.

9.3 Revizuirile intermediare pot fi declanșate și de:

9.3.1 achiziția sau cesionarea unor unități de business

9.3.2 schimbări de furnizor care afectează activele administrate de terți

9.3.3 modernizări tehnologice care implică dezafectare sau alocare la scară largă

9.4 Toate reviziile acestei politici trebuie:

9.4.1 să fie supuse controlului versiunilor și stocate în depozitul SMSI

9.4.2 să fie aprobate de conducerea executivă

9.4.3 să includă un rezumat al modificărilor și justificarea acestora

9.4.4 să fie comunicate tuturor părților interesate afectate, inclusiv procedurile actualizate sau instruirea privind sistemele, acolo unde este aplicabil

10. Politici conexe și corelări

10.1 Această politică funcționează împreună cu următoarele politici conexe și susține aplicarea acestora:

10.1.1 P4 - Politica de control al accesului: Asigură alinierea vizibilității activelor cu drepturile de acces și mecanismele de control din sisteme și medii de date.

10.1.2 P7 - Politica de integrare și încetare a raporturilor de muncă: Reglementează alocarea la timp și returnarea activelor fizice și logice în timpul tranzițiilor de personal.

10.1.3 P13 - Politica de clasificare și etichetare a datelor: Stabilește reguli obligatorii de clasificare pentru active, care determină procedurile de etichetare, gestionare și eliminare.

10.1.4 P14 - Politica de păstrare și eliminare a datelor: Definește termenele și metodele de eliminare securizată pentru activele digitale și fizice care conțin informații.

10.1.5 P22 - Politica de jurnalizare și monitorizare: Permite trasabilitatea accesului la active și a utilizării acestora prin jurnalizarea sistemelor, vizibilitate la nivel de punct terminal și analiză comportamentală.

10.1.6 P30 - Politica de răspuns la incidente: Susține limitarea rapidă a impactului și investigarea incidentelor asociate activelor, cum ar fi laptopurile pierdute sau mediile de stocare neurmărite.

10.2 Aceste politici formează o structură coerentă de guvernanță care asigură gestionarea securizată a activelor, inventarierea exactă și administrarea adecvată a acestora pe întreg ciclul de viață.

11. Standarde și cadre de referință

11.1 Această politică este aliniată la standarde recunoscute internațional în domeniul securității informațiilor și la cadre de reglementare care impun un management robust al activelor pe întreg ciclul de viață.

11.2 ISO/IEC 27001:

11.2.1 Clauza 8.1 - Impune organizațiilor să planifice, să implementeze și să controleze procesele necesare pentru îndeplinirea cerințelor de securitate a informațiilor, inclusiv a celor privind gestionarea ciclului de viață al activelor.

11.3 ISO/IEC 27002:2022 - Controalele 5.9-5.11

11.3.1 Controlul 5.9 - Inventarul informațiilor și al altor active asociate: Impune existența unui inventar actualizat și complet al tuturor activelor relevante pentru prelucrarea informațiilor.

11.3.2 Controlul 5.10 - Utilizarea acceptabilă a activelor: Este susținut prin reguli de utilizare, proprietate și procese de returnare.

11.3.3 Controlul 5.11 - Returnarea activelor: Este implementat prin proceduri formale de predare și dezafectare.

11.3.4 Aceste controale stabilesc cerințe structurate pentru identificarea, etichetarea, menținerea și urmărirea activelor organizației, împreună cu responsabilități corespunzătoare pentru proprietari și custozi pe întreg ciclul de viață.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Inventarul componentelor de sistem: Se reflectă prin management centralizat al activelor, vizibilitate în timp real și corelare cu configurațiile operaționale.

11.4.2 RA-3 - Evaluarea riscurilor: Inventarele de active reprezintă elemente fundamentale pentru modelarea amenințărilor și evaluarea riscurilor.

11.4.3 MP-6 - Sanitizarea mediilor: Este aplicată prin metode de eliminare securizată definite în controalele ciclului de viață al activelor și în politica de eliminare a datelor.

11.5 GDPR al UE (2016/679):

11.5.1 Articolul 30 - Evidențe ale activităților de prelucrare: Impune organizațiilor să documenteze sistemele, dispozitivele și depozitele care stochează sau prelucrează date cu caracter personal.

11.5.2 Articolul 32 - Securitatea prelucrării: Este aliniat cu evaluarea riscurilor bazată pe active și cu măsuri de protecție adaptate activelor clasificate și infrastructurii critice.

11.6 Directiva NIS2 a UE (2022/2555):

11.6.1 Articolul 21(2)(a, b): Impune vizibilitatea activelor și inventarierea acestora ca elemente fundamentale pentru analiza riscului, protecție și răspunsul la incidente de securitate cibernetică.

11.6.2 Articolul 21(3): Consolidează necesitatea unei guvernanțe structurate a activelor ca parte a unei culturi organizaționale orientate către securitate.

11.7 Regulamentul DORA al UE (2022/2554):

11.7.1 Articolul 5 - Guvernanță TIC și control intern: Impune entităților financiare să controleze activele TIC prin cerințe clare privind inventarierea, proprietatea și protecția.

11.7.2 Articolul 9 - Cadrul de management al riscurilor TIC: Stabilește că procesele de management al activelor trebuie să susțină atenuarea amenințărilor, planificarea continuității și reziliența serviciilor.

11.8 COBIT 2019:

11.8.1 BAI09 - Gestionarea activelor: Este aliniat direct cu identificarea, clasificarea, utilizarea și eliminarea structurată a activelor organizației.

11.8.2 DSS01 - Operațiuni gestionate: Susține implementarea controalelor care asigură protecția activelor și guvernanța operațională continuă.

11.8.3 MEA03 - Monitorizarea, evaluarea și aprecierea conformității: Asigură auditarea periodică a controalelor de management al activelor și a eficacității acestora în raport cu cerințele de reglementare.