					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P12S					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**

Aliniere la standarde și reglementări

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 8	Cerințe privind managementul activelor
ISO/IEC 27002:2022	Controlul 5	Controale privind managementul activelor
NIST SP 800-53 Rev.5	CM-8	Inventarul componentelor sistemului
Directiva UE NIS2	Articolul 21 alineatul (2) litera (a)	Evidența activelor pentru protecția rețelelor și a sistemelor informatice
Regulamentul UE DORA	Articolul 5 alineatul (8)	Cerințe privind inventarul activelor TIC
COBIT 2019	BAI	Managementul activelor IT pe întreg ciclul de viață
GDPR	Articolul 30	Evidența activităților de prelucrare a datelor

1. Scop

1.1 Această politică definește modul în care organizația identifică, urmărește, protejează și scoate din uz activele sale informaționale, inclusiv componentele fizice și digitale.

1.2 Scopul este reducerea riscurilor operaționale și de securitate prin menținerea vizibilității, a responsabilității și a gestionării securizate a tuturor activelor organizației pe întreg ciclul lor de viață.

1.3 Un inventar al activelor fiabil sprijină conformitatea cu reglementările, răspunsul la incidente, planificarea continuității activității și procesul de management al riscurilor.

1.4 Această politică sprijină, de asemenea, certificarea conform ISO/IEC 27001 și demonstrează alinierea la obligațiile legale, financiare și de securitate cibernetică prevăzute de cadre precum GDPR, NIS2 și DORA.

1.5 Pentru întreprinderile mici și mijlocii (IMM-uri), o abordare simplă, dar sistematică, a managementului activelor este esențială pentru a evita dispozitivele negestionate, pierderile de date sau neconformitățile identificate în audit, în special atunci când resursele tehnice și de personal sunt limitate.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor activelor deținute, închiriate sau administrate în orice alt mod de organizație, inclusiv celor utilizate în:

2.1.1 activitatea de birou

2.1.2 regim de lucru la distanță sau hibrid

2.1.3 activități de teren sau operațiuni mobile

2.1.4 medii cloud și externalizate

2.2 Tipurile de active acoperite includ, fără a se limita la:

2.2.1 Hardware: laptopuri, desktopuri, monitoare, telefoane, tablete, unități USB, routere, imprimante, medii de backup

2.2.2 Software: aplicații instalate, servicii SaaS, sisteme de operare, soluții antivirus, licențe

2.2.3 Active de date: depozite de date de business, foi de calcul, înregistrări privind clienții, cod sursă

2.2.4 Credențiale și servicii digitale: nume de domeniu, certificate digitale, chei API, conturi de e-mail, credențiale de autentificare pentru cloud

2.2.5 Dispozitive de acces: chei, carduri inteligente, ecusoane de acces, tokenuri biometrice

2.3 Toți angajații, contractanții și furnizorii terți care gestionează activele organizației intră în domeniul de aplicare al acestei politici.

2.4 Politica reglementează, de asemenea, atât activele pe termen scurt (de exemplu, laptopuri dedicate unui proiect), cât și activele pe termen lung, precum și activele partajate utilizate de mai mulți membri ai personalului.

3. Obiective

3.1 Stabilirea și menținerea unui inventar al activelor complet și exact pentru toate activele relevante, actualizat în mod continuu.

3.2 Asigurarea faptului că fiecare activ are un proprietar desemnat, responsabil pentru utilizarea, stocarea și returnarea acestuia.

3.3 Clasificarea activelor în funcție de sensibilitate, impactul asupra activității sau relevanța de reglementare, pentru a permite niveluri diferențiate de protecție.

3.4 Definirea unor proceduri clare pentru alocarea activelor, realocare, mentenanță, raportarea pierderilor și scoaterea din uz.

3.5 Asigurarea faptului că activele sunt gestionate în condiții de securitate pe întreg ciclul lor de viață și că informațiile pe care le stochează sunt fie protejate, fie șterse în mod securizat la eliminare.

3.6 Reducerea probabilității producerii unor incidente de securitate cauzate de resurse organizaționale neurmărite, nereturnate sau utilizate necorespunzător.

3.7 Sprijinirea conformității cu legislația aplicabilă (de exemplu, principiul responsabilității din GDPR) și cu standardele de certificare în domeniul securității cibernetice.

4. Roluri și responsabilități

4.1 Directorul general

4.1.1 Este titularul acestei politici și răspunde de asigurarea faptului că practicile de management al activelor sunt implementate și respectate la nivelul întregii organizații.

4.1.2 Revizuiește și aprobă actualizările inventarului activelor și autorizează scoaterea din uz sau transferul activelor, după caz.

4.1.3 Trebuie informat cu privire la orice pierdere semnificativă, furt sau utilizare necorespunzătoare a activelor.

4.2 Responsabilul IT sau custodele de active desemnat

4.2.1 Menține inventarul activelor (de exemplu, într-o foaie de calcul, într-un sistem de ticketing sau într-un instrument simplificat de evidență a activelor).

4.2.2 Atribuie proprietatea asupra activelor și urmărește schimbările de statut (de exemplu, nou, în utilizare, în reparație, scos din uz).

4.2.3 Verifică faptul că toate activele alocate sunt documentate și asociate unei persoane sau unei unități de business.

4.2.4 Asigură aplicarea și respectarea etichetelor de clasificare (de exemplu, Intern, Confidențial).

4.2.5 Coordonează recuperarea, sanitizarea și dezactivarea activelor în cadrul încetării colaborării sau la scoaterea din uz.

4.2.6 Raportează Directorului general orice neconcordanțe privind activele care nu au fost soluționate.

[... 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 o dată pe an și ori de câte ori:

9.1.1 sunt introduse noi tipuri de tehnologie sau active

9.1.2 se modifică procedurile de urmărire a activelor (de exemplu, prin adoptarea de noi instrumente sau platforme)

9.1.3 noi obligații de reglementare afectează trasabilitatea sau eliminarea activelor

9.1.4 un incident sau un audit identifică o lacună în practicile curente de management al activelor

9.2 Revizuirile trebuie să implice Directorul general și responsabilul IT și să includă actualizări ale procedurilor de gestionare a activelor, ale modelelor de inventar și ale ghidului de clasificare.

9.3 Toate actualizările trebuie documentate și comunicate personalului afectat. Un registru al modificărilor, supus controlului versiunilor, trebuie păstrat.

10. Politici conexe și corelări

10.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: stabilește responsabilitatea pentru deținerea politicilor și pentru operațiunile IT.

10.2 P4S – Politica de control al accesului: corelează utilizarea activelor (de exemplu, laptopuri, dispozitive mobile) cu drepturile de acces ale utilizatorilor și cu managementul identității și accesului.

10.3 P7S – Politica de integrare și încetare a raporturilor de muncă: asigură integrarea alocării și recuperării activelor în procesele aferente ciclului de viață al personalului.

10.4 P13S – Politica de clasificare și etichetare a datelor: stabilește regulile pentru determinarea situațiilor în care un activ trebuie clasificat ca Intern sau Confidențial.

10.5 P30S – Politica de răspuns la incidente: stabilește procedurile de răspuns dacă un eveniment legat de active conduce la o încălcare a securității sau a confidențialității.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1: impune controale operaționale pentru gestionarea activelor și protejarea acestora pe întreaga durată a utilizării.

11.2 ISO/IEC 27002

11.2.1 Controlul 5.9: detaliază modul de identificare, atribuire a proprietății, clasificare și gestionare securizată a activelor.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-8: impune organizațiilor să elaboreze și să mențină un inventar al componentelor sistemului, inclusiv active hardware, software și virtuale.

11.4 GDPR

11.4.1 Articolul 30: impune documentarea activităților de prelucrare a datelor, ceea ce depinde de cunoașterea locului în care sunt stocate datele și a activelor pe care acestea se află.

11.5 Directiva UE NIS2

11.5.1 Articolul 21 alineatul (2) litera (a): prevede măsuri tehnice și organizaționale, inclusiv evidența activelor, pentru protejarea rețelelor și a sistemelor informatice.

11.6 Regulamentul UE DORA

11.6.1 Articolul 5 alineatul (8): entitățile financiare trebuie să mențină inventare detaliate ale activelor TIC ca parte a managementului riscurilor TIC.

11.7 COBIT 2019

11.7.1 BAI09: specifică faptul că activele IT trebuie gestionate pe întreg ciclul lor de viață — de la achiziție până la scoaterea din uz — cu proprietate clar definită și controale adecvate.