					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P13					Titlul documentului: **Politica de clasificare și etichetare a datelor**							
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 Prezenta politică definește cadrul formal pentru clasificarea și etichetarea activelor informaționale ale organizației, pe baza sensibilității, a expunerii la risc și a obligațiilor de reglementare.

1.2 Aceasta asigură că toate informațiile — indiferent dacă sunt stocate, transmise sau prelucrate — sunt clasificate și etichetate în mod clar, astfel încât să indice nivelul necesar de protecție și de gestionare.

1.3 Politica impune o clasificare structurată, aliniată cu practicile organizației de management al riscurilor, și susține obiectivele de confidențialitate, integritate și disponibilitate (CIA) pentru datele aflate atât în format digital, cât și fizic.

1.4 Acest control este esențial pentru a permite controale de acces bazate pe roluri, pregătirea pentru audit, partajarea adecvată a datelor și implementarea eficace a măsurilor tehnice de protecție, precum criptarea, copiile de siguranță și monitorizarea.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică:

2.1.1 Tuturor activelor informaționale ale organizației, inclusiv documentelor, bazelor de date, înregistrărilor și comunicațiilor

2.1.2 Tuturor formatelor de date, inclusiv digitale, tipărite, scrise sau verbale

2.1.3 Tuturor mediilor: la sediu, la distanță, mobile și cloud

2.1.4 Tuturor angajaților, contractanților, furnizorilor de servicii și terților împuterniciți care creează, gestionează sau stochează informațiile organizației

2.2 Domeniul de aplicare include conținut dezvoltat intern, date obținute din surse externe, date cu caracter personal supuse obligațiilor prevăzute de legislația privind protecția datelor (de exemplu, GDPR), precum și informații schimbate cu clienți, parteneri și autorități de reglementare.

2.3 Aceasta se aplică tuturor sistemelor utilizate pentru stocarea sau transmiterea datelor, inclusiv aplicațiilor enterprise, serverelor de fișiere, sistemelor de e-mail, platformelor cloud și depozitelor de backup.

3. Obiective

3.1 Stabilirea unei scheme standardizate de clasificare la nivelul întregii organizații, bazate pe impactul expunerii sau compromiterii datelor.

3.2 Asigurarea faptului că toate informațiile sunt etichetate în mod vizibil și persistent, pentru a reflecta nivelul lor de clasificare și cerințele de gestionare.

3.3 Impunerea controalelor de gestionare a datelor și de acces aliniate clasificării, inclusiv criptare, jurnalizare, protecția transmiterii și definirea perioadelor de păstrare.

3.4 Sprijinirea conformității cu standardele internaționale (ISO/IEC 27001, 27002), cadrele legale (GDPR, NIS2, DORA) și politicile interne de risc.

3.5 Asigurarea faptului că toți utilizatorii își înțeleg responsabilitățile privind protejarea datelor, aplicarea etichetelor și gestionarea corectă a informațiilor clasificate.

3.6 Menținerea trasabilității între statutul clasificării, controalele asociate și Inventarul activelor organizației, în scopuri de audit și conformitate.

4. Roluri și responsabilități

4.1 Directorul de securitate a informațiilor (CISO)

4.1.1 Este proprietarul politicii de clasificare și etichetare a informațiilor și se asigură că aceasta este aliniată la cerințele de reglementare, contractuale și operaționale.

4.1.2 Aprobă nivelurile de clasificare, standardele de etichetare și revizuirile politicii.

4.1.3 Asigură supravegherea conformității cu politica prin audituri, indicatori și revizuirea excepțiilor.

4.1.4 Coordonează guvernanța transversală cu echipele juridice, de protecție a datelor și de risc.

4.2 Proprietarii informațiilor

4.2.1 Sunt responsabili pentru clasificarea activelor informaționale aflate sub controlul lor, utilizând schema de clasificare a organizației.

4.2.2 Aplică etichetele de clasificare la momentul creării, actualizării sau preluării informațiilor.

4.2.3 Revizuiesc periodic clasificarea activelor, în special ca răspuns la modificări ale sensibilității, ale domeniului de reglementare sau ale valorii pentru organizație.

4.2.4 Se asigură că datele sensibile sunt gestionate și etichetate corespunzător pe întreg ciclul lor de viață.

[... 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 Prezenta politică trebuie revizuită cel puțin anual pentru a asigura alinierea cu:

9.1.1 Cerințele de reglementare în evoluție (de exemplu, GDPR, NIS2, DORA)

9.1.2 Actualizările ghidurilor ISO/IEC 27001 sau 27002 privind clasificarea

9.1.3 Schimbările organizaționale care afectează sensibilitatea datelor sau dreptul de proprietate asupra acestora

9.1.4 Schimbările tehnologice, inclusiv noile platforme de management al documentelor sau datelor

9.2 Directorul de securitate a informațiilor (CISO) trebuie să inițieze revizuirea în colaborare cu Comitetul de securitate a informațiilor, consilierul juridic și unitățile de business afectate.

9.3 Revizuirile trebuie să includă:

9.3.1 Eficacitatea aplicării clasificării și respectarea cerințelor de către utilizatori

9.3.2 Analiza incidentelor sau excepțiilor asociate clasificării eronate

9.3.3 Feedbackul utilizatorilor privind instrumentele de etichetare sau materialele de îndrumare

9.3.4 Analiza comparativă cu standardele de clasificare din industrie

9.4 Actualizările politicii trebuie să fie supuse controlului versiunilor, documentate în depozitul SMSI și comunicate întregului personal relevant, cu accent pe noile responsabilități sau schimbările de instrumente.

9.5 Personalul nou-angajat trebuie informat cu privire la versiunea curentă a politicii în cadrul procesului de integrare. Toți angajații trebuie să finalizeze instruirea de reîmprospătare după modificări semnificative ale politicii.

10. Politici conexe și corelări

10.1 Prezenta politică este susținută în mod direct de și aplică controalele descrise în următoarele politici conexe:

10.1.1 P4 - Politica de control al accesului: accesul la informații este guvernat de nivelurile de clasificare; datele mai sensibile necesită mecanisme mai stricte de control al accesului și autorizare.

10.1.2 P11 - Politica de management al conturilor de utilizator și al privilegiilor: consolidează alocarea privilegiilor pe baza principiului necesității de a cunoaște, determinat de nivelurile de clasificare.

10.1.3 P12 - Politica de management al activelor: asigură că fiecare activ din inventar include clasificarea și eticheta sa, sprijinind trasabilitatea și responsabilizarea.

10.1.4 P14 - Politica de păstrare și eliminare a datelor: regulile de păstrare și eliminare sunt determinate de nivelul de clasificare al datelor și de obligațiile de păstrare impuse de reglementări.

10.1.5 P18 - Politica privind controalele criptografice: aplică standarde de criptare adecvate pe baza clasificării activului informațional.

10.1.6 P22 - Politica de jurnalizare și monitorizare: permite monitorizarea accesului la informații clasificate și a circulației acestora, asigurând verificabilitatea pentru audit și detectarea etichetării eronate sau a utilizării necorespunzătoare.

10.2 Fiecare corelare asigură protecția consecventă a informațiilor pe întreg ciclul lor de viață, de la creare și clasificare până la gestionare securizată, stocare, transmitere și distrugere finală.

11. Standarde și cadre de referință

11.1 Prezenta politică este aliniată cu standarde și cadre de reglementare recunoscute la nivel internațional, care guvernează clasificarea și etichetarea informațiilor sensibile.

11.2 ISO/IEC 27001

11.2.1 Clauza 4.2 - Înțelegerea nevoilor și a așteptărilor părților interesate. Cerințele de clasificare derivă adesea din obligații legale, de reglementare sau contractuale impuse de părțile interesate (de exemplu, GDPR, acorduri de confidențialitate (NDA) cu clienții), care trebuie reflectate în politică.

11.2.2 Clauza 6.1.3 - Tratamentul riscului de securitate a informațiilor. Clasificarea influențează direct selectarea controalelor de tratare a riscului, inclusiv controlul accesului, criptarea și păstrarea, în funcție de sensibilitatea datelor.

11.2.3 Clauza 7.2 - Competență. Politica impune ca personalul responsabil pentru clasificare și etichetare să fie instruit, ceea ce se încadrează în cerințele privind competența.

11.2.4 Clauza 7.3 - Conștientizare. Politica prevede că toți utilizatorii trebuie să cunoască nivelurile de clasificare și responsabilitățile lor privind gestionarea informațiilor, în concordanță cu obligațiile de conștientizare.

11.2.5 Clauza 7.5 - Informații documentate. Politica de clasificare în sine este un document controlat, iar procedurile, înregistrările de instruire și etichetele de clasificare fac parte din informațiile documentate.

11.2.6 Clauza 8.1 - Planificare și control operațional. Clasificarea și etichetarea sunt procese operaționale integrate în managementul ciclului de viață al datelor, iar această clauză asigură că astfel de activități sunt planificate, implementate și controlate.

11.2.7 Clauza 9.1 - Monitorizare, măsurare, analiză și evaluare. Politica include prevederi pentru monitorizarea conformității clasificării, a tendințelor privind incidentele și a eficacității schemei de etichetare.

11.2.8 Clauza 10.1 - Neconformitate și acțiune corectivă. Politica definește răspunsurile la clasificarea eronată, inclusiv acțiuni corective precum reinstruirea, actualizările și gestionarea excepțiilor.

11.3 ISO/IEC 27002:2022

11.3.1 Controlul 5.12 - Clasificarea informațiilor. Acest control asigură că informațiile sunt clasificate în funcție de sensibilitatea, valoarea și criticitatea lor — exact ceea ce formalizează prezenta politică.

11.3.2 Controlul 5.13 - Etichetarea informațiilor. Acest control impune etichetarea adecvată a informațiilor în conformitate cu nivelul lor de clasificare, aspect tratat integral în politică.

11.3.3 Controlul 5.10 - Utilizarea acceptabilă a informațiilor și a altor active asociate. Politica impune modul în care utilizatorii trebuie să gestioneze datele clasificate, sprijinind direct utilizarea acceptabilă și prevenind utilizarea necorespunzătoare.

11.3.4 Controlul 5.11 - Returnarea activelor. Clasificarea contribuie la identificarea datelor sensibile și la returnarea sau sanitizarea lor în condiții de securitate atunci când un angajat sau un furnizor pleacă.

11.3.5 Controlul 5.9 - Inventarul informațiilor și al altor active asociate. Clasificarea este adesea corelată cu Inventarul activelor, care trebuie să reflecte nivelul de clasificare al fiecărui element pentru a sprijini alocarea corespunzătoare a controalelor.

11.3.6 Controlul 5.14 - Transferul informațiilor. Nivelurile de clasificare influențează controalele privind transferurile interne și externe de date (de exemplu, criptare, aprobare, restricții de acces).

11.3.7 Controlul 8.12 - Prevenirea scurgerilor de date. Aplicarea clasificării și etichetării sprijină prevenirea divulgării neautorizate și a pierderii datelor.

11.3.8 Controlul 8.11 - Mascarea datelor. Anumite niveluri de clasificare (de exemplu, Confidențial, Restricționat) pot impune mascarea atunci când datele sunt utilizate în testare/dezvoltare sau analiză.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Politica și procedurile privind protecția sistemelor și comunicațiilor: sprijină politicile de clasificare ca parte a protecției generale a datelor.

11.4.2 AC-16 - Atribute de securitate: implementează aplicarea accesului pe baza metadatelor de clasificare și a permisiunilor utilizatorilor.

11.4.3 MP-3 / MP-5 - Marcarea mediilor și protecția în tranzit: impun etichetarea și protecția datelor în repaus și în tranzit în funcție de clasificare.

11.5 GDPR al UE (2016/679)

11.5.1 Articolul 5 - Principiile protecției datelor: impune ca datele cu caracter personal să fie prelucrate în condiții de securitate, proporțional cu sensibilitatea lor.

11.5.2 Articolul 32 - Securitatea prelucrării: consolidează clasificarea ca mecanism de protecție a datelor bazat pe risc și de aplicare a măsurilor tehnice adecvate.

11.6 Directiva NIS2 a UE (2022/2555)

11.6.1 Articolul 21(2)(a): impune politici pentru managementul riscurilor de securitate a informațiilor, inclusiv controale pentru clasificarea activelor și a datelor.

11.6.2 Articolul 21(3): încurajează adoptarea de măsuri pentru aplicarea gestionării adecvate a datelor — susținută prin etichetare bazată pe clasificare.

11.7 Regulamentul DORA al UE (2022/2554)

11.7.1 Articolul 5 - Guvernanță și control: impune cadre de guvernanță care clasifică activele de date pentru controlul riscurilor TIC.

11.7.2 Articolul 9 - Managementul riscurilor TIC: impune măsuri tehnice și organizatorice pentru activele TIC critice, inclusiv clasificarea și etichetarea.

11.8 COBIT 2019

11.8.1 DSS05.02 - Gestionarea serviciilor de securitate: impune clasificări de securitate a informațiilor pentru a asigura protecția datelor organizației.

11.8.2 MEA03 - Monitorizarea, evaluarea și aprecierea conformității: sprijină auditul și revizuirea periodică a practicilor de clasificare pentru a asigura respectarea politicii și maturitatea.