					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P13S					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**

Aliniere la standarde și reglementări, după caz

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 5.3, 8	
ISO/IEC 27002:2022	Controalele 5.12, 5.13	
NIST SP 800-53 Rev. 5	AC-16, MP-3, MP-5	
Directiva UE NIS2	Articolul 21 alineatul (2) litera (a)	
Regulamentul UE DORA	Articolul 5 alineatul (8)	
COBIT 2019	BAI03.05, DSS05	
GDPR	Articolele 5, 32	

1. Scop

1.1 Prezenta politică stabilește modul în care toate informațiile gestionate de organizație trebuie clasificate și etichetate pentru a asigura menținerea confidențialității, integrității și disponibilității (CIA) pe întregul lor ciclu de viață.

1.2 Aceasta permite gestionarea consecventă a datelor prin atribuirea unor niveluri adecvate de protecție informațiilor, în funcție de sensibilitate, impactul asupra activităților organizației sau obligațiile legale.

1.3 Clasificarea și etichetarea contribuie la reducerea riscului de divulgare accidentală a informațiilor, acces neautorizat sau gestionare necorespunzătoare a datelor sensibile, în special în cadrul IMM-urilor care se pot baza pe sisteme mai simple și pe controale mai puțin formalizate.

1.4 Prezenta politică este esențială pentru certificarea ISO/IEC 27001 și pentru conformitatea cu reglementările, în special cu legislația privind protecția datelor, precum GDPR, și cu cadrele de securitate cibernetică, precum NIS2 și DORA.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor datelor organizației, indiferent de format sau locație, inclusiv:

2.1.1 documente electronice, foi de calcul, e-mailuri, formulare, imagini și fișiere scanate;

2.1.2 documente fizice, precum evidențe tipărite, rapoarte, facturi și notițe;

2.1.3 date stocate sau prelucrate în servicii cloud, pe servere locale, pe medii amovibile sau pe dispozitive personale utilizate în scop profesional;

2.1.4 date temporare sau tranzitorii generate în cursul activităților operaționale ale organizației (de exemplu, jurnale, fișiere cache, e-mailuri).

2.2 Întregul personal, contractanții, lucrătorii temporari și furnizorii externi care au acces la datele organizației trebuie să respecte prezenta politică.

2.3 Aceasta se aplică pe întregul ciclu de viață al datelor — de la creare și stocare, trecând prin acces și transfer, până la arhivare sau ștergere.

3. Obiective

3.1 Să definească o schemă de clasificare simplă și aplicabilă, care poate fi înțeleasă și utilizată cu ușurință în întreaga organizație.

3.2 Să impună clasificarea fiecărui activ de date în funcție de sensibilitatea sa și etichetarea corespunzătoare, pentru a ghida gestionarea, stocarea și accesul adecvate.

3.3 Să asigure integrarea practicilor de etichetare a datelor în fluxurile de lucru ale organizației, precum integrarea personalului, inițierea proiectelor și configurarea sistemelor.

3.4 Să reducă riscul de încălcare a securității datelor prin aplicarea unor controale de protecție (de exemplu, criptare, restricționarea accesului) în funcție de nivelul de clasificare.

3.5 Să asigure conformitatea cu legislația privind confidențialitatea și securitatea informațiilor, demonstrând că datele sensibile (de exemplu, date cu caracter personal, financiare sau proprietare) sunt etichetate și gestionate corespunzător.

3.6 Să stabilească responsabilitatea pentru deciziile de clasificare și să asigure revizuiri și actualizări periodice în funcție de evoluția nevoilor organizației și a cerințelor legale.

4. Roluri și responsabilități

4.1 Director general

4.1.1 Deține prezenta politică și aprobă schema de clasificare.

4.1.2 Asigură supravegherea pentru a se asigura că responsabilitățile privind clasificarea sunt delegate și aplicate.

4.1.3 Revizuiește și autorizează orice excepție de la cerințele de clasificare sau etichetare.

4.1.4 Se asigură că practicile de gestionare a datelor respectă cerințele de conformitate prevăzute de acte normative precum GDPR și DORA.

4.2 Proprietarul informației / managerul de date

4.2.1 Atribuie o clasificare inițială fiecărui set nou de date sau activ informațional la creare sau achiziție.

4.2.2 Se asigură că sunt aplicate etichete vizibile, după caz (de exemplu, antete de fișier, subsoluri, filigrane, denumiri de foldere).

4.2.3 Revizuiește periodic clasificările pentru a verifica relevanța, acuratețea și eventualele modificări necesare (de exemplu, după declasificare sau publicare).

4.2.4 Colaborează cu responsabilul IT pentru a aplica măsuri de protecție tehnice în funcție de clasificare (de exemplu, drepturi de acces, criptare).

[... 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 anual de către Directorul general și managerul de date pentru a se asigura că reflectă:

9.1.1 modificări ale activităților operaționale ale organizației sau ale tipurilor de date;

9.1.2 noi cerințe de reglementare (de exemplu, privind confidențialitatea datelor sau supravegherea financiară);

9.1.3 schimbări tehnologice care afectează capabilitățile de etichetare sau clasificare.

9.2 Revizuirea trebuie să includă actualizări ale categoriilor de clasificare, ale instrumentelor sau practicilor de etichetare și ale conținutului de conștientizare și instruire.

9.3 Revizuirile politicii trebuie aprobate de Directorul general și comunicate întregului personal. O evidență a modificărilor de versiune trebuie păstrată în scopuri de audit.

10. Politici conexe și corelări

10.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: stabilește responsabilitatea pentru deținerea și aplicarea politicii.

10.2 P4S – Politica de control al accesului: aliniază accesul la sisteme cu nivelurile de clasificare a datelor.

10.3 P12S – Politica de management al activelor: urmărește activele fizice și digitale care stochează date clasificate.

10.4 P17S – Politica de protecție a datelor și confidențialitate: reglementează protecția datelor cu caracter personal, dintre care o mare parte sunt clasificate ca fiind Confidențiale.

10.5 P30S – Politica de răspuns la incidente: definește căile de escaladare și procedurile de răspuns în caz de încălcări ale clasificării sau de expunere a datelor.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 5.3: impune definirea clară a responsabilităților pentru gestionarea și protecția datelor.

11.1.2 Clauza 8.1: impune planificarea și controalele operaționale, inclusiv pe cele asociate clasificării datelor.

11.2 ISO/IEC 27002

11.2.1 Controlul 5.12: oferă îndrumări privind clasificarea informațiilor pe baza riscului și a cerințelor de reglementare.

11.2.2 Controlul 5.13: detaliază mecanisme practice de etichetare și regulile de gestionare asociate.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-16: impune marcarea informațiilor pentru a se asigura că măsurile de protecție sunt aliniate cu clasificarea.

11.3.2 MP-3 / MP-5: oferă îndrumări privind etichetarea și controlul mediilor de stocare și al rezultatelor.

11.4 GDPR

11.4.1 Articolele 5 și 32: impun reducerea la minimum a datelor și asigurarea integrității prin măsuri adecvate de clasificare și gestionare.

11.5 Directiva UE NIS2

11.5.1 Articolul 21 alineatul (2) litera (a): impune controale tehnice și organizatorice pentru protecția datelor bazată pe risc.

11.6 Regulamentul UE DORA

11.6.1 Articolul 5 alineatul (8): impune organizațiilor să clasifice activele de date ca parte a programului lor de management al riscurilor TIC.

11.7 COBIT 2019

11.7.1 BAI03.05: prevede clasificarea informațiilor și protecția ajustată în funcție de risc.

11.7.2 DSS05.02: abordează aplicarea controalelor bazate pe clasificare și monitorizarea acestora.