					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P14S					Titlul documentului: **Politica de retenție și eliminare 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

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 6.1.3, 8	Acoperă tratarea riscurilor, controalele operaționale și cerințele de retenție
ISO/IEC 27002:2022	Controlul 5	Oferă îndrumări privind perioadele de retenție și metodele de distrugere securizată
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Păstrarea jurnalelor de audit, sanitizarea mediilor de stocare, limitele de retenție a datelor și aplicarea acestora
Directiva UE NIS2	Articolul 21(2)(a)	Este necesară o politică de management al ciclului de viață adecvată riscurilor
Regulamentul UE DORA	Articolul 5(1)	Managementul riscurilor TIC: disponibilitatea și eliminarea datelor
COBIT 2019	BAI03.04, DSS01	Controale pentru ciclul de viață al informației, eliminare securizată
RGPD al UE	Articolul 5(1)(e), 17	Datele nu trebuie păstrate mai mult decât este necesar; dreptul la ștergere

1. Scop

1.1 Scopul acestei politici este de a defini reguli obligatorii pentru retenția și eliminarea securizată a informațiilor într-un mediu specific IMM-urilor. Aceasta asigură că înregistrările sunt păstrate doar pe durata impusă de lege, de obligațiile contractuale sau de necesitățile operaționale ale organizației, iar ulterior sunt distruse în mod securizat.

1.2 Această politică urmărește reducerea riscului informațional, gestionarea expunerii juridice și limitarea stocării datelor redundante sau învechite. Politica sprijină conformitatea cu ISO/IEC 27001 și cu cadrele de protecție a datelor, precum RGPD, prin reducerea păstrării neautorizate a informațiilor cu caracter personal sau sensibile.

1.3 Un cadru de retenție și eliminare bine structurat reduce costurile operaționale, îmbunătățește performanța sistemelor și crește gradul de pregătire pentru audit. Pentru IMM-urile cu o capacitate IT limitată, acesta oferă o modalitate practică de a gestiona în mod responsabil activele informaționale în format digital și fizic.

2. Domeniu de aplicare

2.1 Această politică se aplică:

2.1.1 tuturor înregistrărilor, fișierelor, jurnalelor, comunicărilor și seturilor de date create, colectate, prelucrate sau stocate de organizație;

2.1.2 tuturor angajaților, contractanților și furnizorilor externi care gestionează datele organizației;

2.1.3 tuturor formatelor de date (de exemplu, hârtie, format electronic, imagine, audio sau jurnal) și tuturor mediilor de stocare (de exemplu, unități locale, servicii cloud, servere de e-mail, copii de rezervă).

2.2 Domeniul de aplicare include:

2.2.1 documente de afaceri (de exemplu, facturi, contracte, rapoarte de proiect);

2.2.2 înregistrări operaționale (de exemplu, jurnale, istoric de acces, instantanee de backup);

2.2.3 date cu caracter personal (de exemplu, fișiere de resurse umane, comunicări cu clienții, înregistrări de suport);

2.2.4 date găzduite intern, extern sau în medii hibride;

2.2.5 date arhivate și date din copiile de rezervă, indiferent dacă sunt active sau inactive.

2.3 Toate etapele ciclului de viață al datelor intră în domeniul de aplicare, de la creare până la eliminarea autorizată.

3. Obiective

3.1 Să definească reguli de retenție consecvente, bazate pe criterii juridice, operaționale și de reglementare.

3.2 Să prevină ștergerea prematură a înregistrărilor critice și să elimine acumularea inutilă de date.

3.3 Să asigure eliminarea securizată și ireversibilă a datelor atunci când retenția nu mai este necesară.

3.4 Să atribuie responsabilitatea pentru aplicarea deciziilor privind retenția și ștergerea, ținând cont de constrângerile de personal specifice IMM-urilor.

3.5 Să furnizeze documentație pregătită pentru audit, pentru a demonstra diligența necesară în raport cu ISO 27001, RGPD, NIS2 și alte cadre aplicabile.

3.6 Să promoveze gestionarea securizată a datelor pe întreg ciclul de viață, fără a impune o povară tehnică inutilă personalului fără specializare.

4. Roluri și responsabilități

4.1 Director general

4.1.1 Aprobă această politică și își asumă responsabilitatea pentru aceasta.

4.1.2 Asigură implementarea procedurilor de retenție și eliminare într-un mod aliniat cu riscul juridic și cu riscul operațional al organizației.

4.1.3 Autorizează excepțiile și măsurile de reținere în scop juridic atunci când este necesar.

4.1.4 Inițiază revizuirea politicii și aprobă actualizările în funcție de schimbările operaționale sau de reglementare.

4.2 Proprietar de date desemnat

4.2.1 Este desemnat pentru fiecare categorie de date (de exemplu, date financiare, resurse umane, înregistrări privind clienții).

4.2.2 Clasifică înregistrările și stabilește perioada de retenție corespunzătoare pe baza politicii și a cerințelor legale aplicabile.

4.2.3 Autorizează ștergerea atunci când cerințele de retenție au fost îndeplinite.

4.2.4 Sprijină auditurile interne prin furnizarea contextului privind raționamentul de retenție și evenimentele de eliminare.

[... 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 sau la apariția oricăreia dintre următoarele situații:

9.1.1 modificări ale legislației aplicabile (de exemplu, protecția datelor, raportare financiară);

9.1.2 adoptarea unor sisteme sau procese noi care afectează ciclul de viață al datelor;

9.1.3 constatări de audit sau incidente care evidențiază lacune în practicile de retenție.

9.2 Revizuirile trebuie să asigure că Registrul de retenție rămâne complet și reflectă toate categoriile majore de înregistrări.

9.3 Actualizările politicii trebuie aprobate de Directorul general și comunicate personalului afectat. Cea mai recentă versiune trebuie să fie accesibilă și supusă controlului versiunilor.

10. Politici conexe și corelări

10.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: definește deținerea politicii și autoritatea pentru excepții.

10.2 P13S – Politica de clasificare și etichetare a datelor: stabilește modul în care regulile de retenție se aliniază la clasificarea datelor.

10.3 P12S – Politica de management al activelor: reglementează mediile de stocare care conțin date supuse retenției și eliminării.

10.4 P17S – Politica de protecție a datelor și confidențialitate: asigură reducerea la minimum a datelor și sprijină prelucrarea legală a informațiilor în temeiul RGPD.

10.5 P30S – Politica de răspuns la incidente: se aplică atunci când deficiențele privind eliminarea sau retenția conduc la o potențială expunere a datelor.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 6.1.3: impune tratarea riscurilor legate de informații, inclusiv a riscurilor de retenție.

11.1.2 Clauza 8.1: definește controalele operaționale pentru ciclul de viață.

11.2 ISO/IEC 27002

11.2.1 Controlul 5.33: oferă îndrumări pentru stabilirea perioadelor de retenție și a metodelor de distrugere securizată.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: impune păstrarea jurnalelor de audit.

11.3.2 MP-6: definește proceduri de sanitizare a mediilor de stocare.

11.3.3 SI-12: abordează limitele de retenție a datelor și aplicarea acestora.

11.4 RGPD al UE

11.4.1 Articolul 5(1)(e): datele trebuie păstrate nu mai mult decât este necesar.

11.4.2 Articolul 17: dreptul la ștergere se aplică atunci când datele nu mai sunt păstrate în mod legal.

11.5 Directiva UE NIS2

11.5.1 Articolul 21(2)(a): impune politici organizaționale adecvate riscurilor, inclusiv pentru managementul ciclului de viață.

11.6 Regulamentul UE DORA

11.6.1 Articolul 5(1): managementul riscurilor TIC include disponibilitatea și eliminarea datelor.

11.7 COBIT 2019

11.7.1 BAI03.04: sunt necesare controale pentru ciclul de viață al informației.

11.7.2 DSS01.06: proceduri de eliminare securizată ca parte a protejării activelor informaționale.