					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P14					Titlul documentului: **Politica de păstrare 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**

Aliniată la standarde și reglementări

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 6.1.3, 8.1	
ISO/IEC 27002:2022	Controalele 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
RGPD al UE	Articolele 5(1)(e), 17, 32	
Directiva NIS2 a UE	Articolul 21(2)(a-e)	
Regulamentul DORA al UE	Articolele 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Scop

1.1 Scopul acestei politici este de a defini cerințele organizaționale privind păstrarea datelor și eliminarea securizată a acestora pe întreg ciclul de viață al informațiilor. Aceasta asigură conformitatea cu obligațiile legale, de reglementare și contractuale aplicabile și previne acumularea inutilă sau riscantă de date.

1.2 Această politică sprijină implementarea ISO/IEC 27001:2022 prin instituirea controlului asupra perioadelor de stocare a datelor și a practicilor de eliminare ireversibilă. Aceasta permite documentarea trasabilă a înregistrărilor, impune perioade de păstrare aliniate la nivelul de sensibilitate și clasificare și asigură pregătirea pentru audit, inspecții de reglementare și proceduri de divulgare legală a informațiilor.

1.3 În plus, politica urmărește să protejeze confidențialitatea, integritatea și disponibilitatea datelor, reducând în același timp riscul organizațional, ineficiențele operaționale și expunerea la încălcări ale confidențialității generate de păstrarea sau distrugerea necorespunzătoare a datelor.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor activelor informaționale fizice și digitale deținute, prelucrate sau păstrate de organizație, inclusiv celor aflate sub controlul unor terți, al filialelor sau al partenerilor de externalizare.

2.2 Domeniul de aplicare include, fără a se limita la:

2.2.1 Documente, fișiere și înregistrări (digitale și pe suport de hârtie)

2.2.2 Baze de date și arhive

2.2.3 E-mailuri și jurnale ale mesajelor instantanee

2.2.4 Copii de siguranță, jurnale de sistem și piste de audit

2.2.5 Cod sursă, date ale aplicațiilor și active găzduite în cloud

2.2.6 Medii amovibile și echipamente scoase din uz care conțin date

2.3 Politica reglementează atât înregistrările operaționale, cât și seturile de date reglementate (de exemplu, conținut financiar, juridic, de resurse umane, referitor la clienți și relevant pentru audit), indiferent de locul de stocare sau de sistem.

2.4 Aceasta se aplică tuturor departamentelor organizației și tuturor angajaților, contractorilor și furnizorilor implicați în crearea, stocarea, administrarea sau eliminarea datelor.

3. Obiective

3.1 Să asigure că datele sunt păstrate numai atât timp cât este necesar din punct de vedere legal, contractual sau operațional și sunt eliminate în condiții de securitate atunci când nu mai sunt necesare.

3.2 Să prevină ștergerea prematură, neautorizată sau accidentală a înregistrărilor necesare pentru operațiuni în curs, conformitate, litigii sau audit.

3.3 Să stabilească și să impună calendare de păstrare consecvente, bazate pe clasificarea informațiilor, tipul activului, cerințele legale aplicabile și expunerea la risc.

3.4 Să protejeze viața privată și confidențialitatea datelor pe durata perioadei de păstrare și la momentul eliminării, inclusiv prin respectarea drepturilor persoanelor vizate (de exemplu, ștergerea în temeiul articolului 17 din RGPD).

3.5 Să asigure că toate metodele de eliminare a datelor sunt ireversibile, documentate corespunzător și conforme cu standarde recunoscute, precum NIST SP 800-88.

3.6 Să reducă ineficiențele operaționale, costurile suplimentare și expunerea juridică generate de păstrarea excesivă sau de datele istorice neinventariate.

3.7 Să sprijine obiectivele de continuitate a activității și de recuperare în caz de dezastru printr-o guvernanță integrată a păstrării copiilor de siguranță și prin practici de arhivare a datelor justificate și demonstrabile.

4. Roluri și responsabilități

4.1 Managementul executiv

4.1.1 Aprobă această politică și asigură finanțarea, resursele și integrarea adecvată în managementul riscurilor la nivelul organizației și în programele de conformitate.

4.1.2 Poartă responsabilitatea generală pentru conformitatea legală și de reglementare aferentă păstrării datelor și eliminării securizate.

4.2 Directorul pentru securitatea informațiilor (CISO)

4.2.1 Deține această politică și este responsabil pentru definirea și revizuirea cadrului de guvernanță privind păstrarea și eliminarea, în aliniere cu ISMS.

4.2.2 Asigură implementarea cerințelor de păstrare și eliminare bazate pe clasificare în cadrul unităților organizaționale și al sistemelor tehnice.

4.2.3 Monitorizează conformitatea cu politica și dispune măsuri corective atunci când este necesar.

[... 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 anual sau atunci când este îndeplinită oricare dintre următoarele condiții:

9.1.1 Modificări ale actelor normative aplicabile care afectează păstrarea datelor (de exemplu, actualizări ale RGPD, ale codurilor fiscale, ale DORA)

9.1.2 Revizuiri ale cadrului de clasificare sau ale proceselor organizației care afectează etapele ciclului de viață al datelor

9.1.3 Introducerea de noi sisteme IT, platforme de arhivare sau tehnologii de eliminare a mediilor de stocare

9.1.4 Constatări ale auditului intern sau recomandări ale autorităților de reglementare care evidențiază lacune în practicile de păstrare sau eliminare

9.2 Revizuirea trebuie coordonată de CISO și de Responsabilul cu protecția datelor (DPO), cu contribuția departamentului juridic, a funcției de conformitate, a IT și a unităților organizaționale.

9.3 Registrul principal al perioadelor de păstrare a datelor (MDRS) și Registrul de eliminare trebuie revizuite în paralel pentru a asigura că:

9.3.1 Calendarele rămân corecte și reflectă nevoile operaționale, legale și de reglementare

9.3.2 Documentația de eliminare este completă și verificabilă

9.3.3 Înregistrările privind măsurile de blocare legală sunt validate și închise atunci când este cazul

9.4 Orice actualizare a politicii trebuie:

9.4.1 Să fie versionată formal și păstrată în depozitul de documente ISMS

9.4.2 Să includă un istoric al reviziilor și justificarea modificărilor

9.4.3 Să fie aprobată de managementul executiv

9.4.4 Să fie comunicată personalului relevant, împreună cu materiale actualizate de instruire sau îndrumare

9.5 În cazul unor modificări semnificative ale politicii, angajații afectați trebuie să finalizeze instruirea specifică în termen de 30 de zile de la publicare, pentru a asigura menținerea conformității.

9.6 Politici conexe și corelări

10. Politici conexe și corelări

10.1.1 P4 - Politica de control al accesului: Asigură că numai persoanele autorizate accesează datele pe durata perioadei de păstrare și că datele expirate sunt restricționate până la eliminare.

10.1.2 P12 - Politica de management al activelor: Identifică activele care conțin date ce necesită eliminare planificată și urmărește ciclul lor de viață de la achiziție până la distrugere.

10.1.3 P13 - Politica de clasificare și etichetare a datelor: Orientează deciziile de clasificare care influențează direct durata de păstrare a datelor și metoda de eliminare necesară.

10.1.4 P15 - Politica de backup și restaurare: Definește perioadele de păstrare și procedurile de eliminare pentru mediile de backup și activele de date replicate.

10.1.5 P18 - Politica controalelor criptografice: Sprijină ștergerea criptografică pentru eliminare și impune criptarea pe durata stocării datelor până la distrugere.

10.1.6 P30 - Politica de răspuns la incidente: Se activează în cazurile în care eliminarea necorespunzătoare generează un potențial de pierdere de date, încălcare a securității sau nerespectare a reglementărilor.

10.2 Fiecare politică asociată contribuie la aplicarea unui model coerent de guvernanță a datelor în ceea ce privește clasificarea, controlul ciclului de viață, accesul și pregătirea pentru audit.

11. Standarde și cadre de referință

11.1 Această politică este aliniată cu standarde recunoscute la nivel global și cu cadre de reglementare care definesc practici sigure, conforme și eficiente pentru ciclul de viață al datelor.

11.2 ISO/IEC 27001:

11.2.1 Clauza 6.1.3 - Plan de tratare a riscurilor: Sprijină reducerea riscurilor asociate păstrării excesive, incidentelor de securitate a datelor sau eșecurilor proceselor de eliminare.

11.2.2 Clauza 8.1 - Planificare și control operațional: Stabilește controale ale ciclului de viață care guvernează stocarea, arhivarea și distrugerea.

11.3 ISO/IEC 27002:2022 - Controalele 5.10, 5.12, 5.30, 5: Oferă îndrumări practice privind utilizarea acceptabilă a datelor, justificarea păstrării, ștergerea controlată și menținerea înregistrărilor într-un mod justificabil, în aliniere cu toleranța la risc a organizației.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Păstrarea înregistrărilor de audit: Asigură stocarea suficientă a jurnalelor de audit și a dovezilor de conformitate.

11.4.2 MP-6 - Sanitizarea mediilor de stocare: Impune metode securizate și documentate de distrugere pentru mediile fizice și electronice.

11.4.3 SI-12 - Gestionarea informațiilor: Impune tratarea adecvată a datelor în aliniere cu controalele de păstrare și eliminare.

11.4.4 PL-2 - Planul de securitate și confidențialitate al sistemului: Impune documentarea, la nivel de sistem, a modului de gestionare a ciclului de viață al datelor și a prevederilor privind eliminarea securizată.

11.5 RGPD al UE (2016/679):

11.5.1 Articolul 5(1)(e) - Minimizarea datelor și limitarea stocării: Impune ca datele să nu fie păstrate mai mult decât este necesar.

11.5.2 Articolul 17 - Dreptul la ștergere („dreptul de a fi uitat”): Impune ștergerea promptă și permanentă a datelor cu caracter personal la o solicitare valabilă.

11.5.3 Articolul 32 - Securitatea prelucrării: Consolidă protecția datelor pe durata păstrării și impune distrugerea securizată a înregistrărilor expirate.

11.6 Directiva NIS2 a UE (2022/2555):

11.6.1 Articolul 21(2)(a-e): Impune entităților adoptarea de politici și măsuri tehnice pentru gestionarea securizată a datelor, inclusiv limitări de stocare și metode de eliminare.

11.7 Regulamentul DORA al UE (2022/2554):

11.7.1 Articolul 5 - Guvernanță și control: Impune un management structurat al riscurilor TIC, inclusiv gestionarea securizată a informațiilor pe întreg ciclul de viață.

11.7.2 Articolul 9 - Cadrul de management al riscurilor TIC: Impune politici privind păstrarea datelor, distrugerea și conformitatea legală și de reglementare a operațiunilor digitale.

11.8 COBIT 2019:

11.8.1 DSS01 - Operațiuni administrate: Sprijină urmărirea păstrării și consecvența între sistemele de date.

11.8.2 DSS05 - Servicii de securitate administrate: Asigură protecția datelor stocate și arhivate până la eliminarea securizată.

11.8.3 MEA03 - Monitorizarea, evaluarea și aprecierea conformității: Permite auditarea aplicării perioadelor de păstrare, a procedurilor de ștergere și a respectării cerințelor de reglementare.