					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P15S					Titlul documentului: **Politica de backup și restaurare**							
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 standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 8	Controale de backup conform cerințelor SMSI
ISO/IEC 27002:2022	Controalele 5.29, 8.13	Bune practici pentru backup și integrarea cu continuitatea activității
NIST SP 800-53 Rev. 5	CP-9, MP-6	Backup și protecția mediilor de backup
Directiva NIS2 a UE	Articolul 21 alineatul (2) litera (c)	Reziliență și continuitate prin backup
Regulamentul DORA al UE	Articolul 10 alineatul (1)	Continuitate TIC – backup pentru organizațiile financiare
COBIT 2019	BAI04.05, DSS04	Documentarea și testarea backup-urilor, procese de control
GDPR al UE	Articolele 5 alineatul (1) litera (f), 32 alineatul (1) litera (c)	Integritatea, disponibilitatea și restaurarea în timp util a datelor

1. Scop

1.1 Prezenta politică definește modul în care organizația efectuează și gestionează backup-urile pentru a asigura continuitatea activității, a proteja împotriva pierderii datelor și a permite recuperarea în timp util în urma incidentelor.

1.2 Aceasta stabilește reguli obligatorii privind efectuarea backup-ului, stocarea și restaurarea sistemelor și datelor, în special în cadrul IMM-urilor fără infrastructură IT complexă.

1.3 Prezenta politică sprijină pregătirea pentru audit și certificarea ISO/IEC 27001, asigurând implementarea controalelor esențiale de backup, aplicarea lor consecventă și revizuirea periodică a acestora.

1.4 Capacitatea organizației de a se recupera în urma defecțiunilor tehnice, a ștergerii accidentale sau a incidentelor cibernetice depinde de respectarea strictă a prezentei politici.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor sistemelor și datelor organizației, inclusiv:

2.1.1 evidențelor financiare, informațiilor despre clienți și datelor de resurse umane

2.1.2 stațiilor de lucru, laptopurilor, serverelor și aplicațiilor cloud utilizate în activitățile operaționale ale organizației

2.1.3 mediilor de backup, precum unități USB, spații de stocare externe sau backup-uri în cloud

2.2 Aceasta se aplică, de asemenea, tuturor persoanelor care au responsabilități privind gestionarea sau operarea proceselor de backup, inclusiv:

2.2.1 Directorului general (DG) sau persoanei desemnate ca responsabil

2.2.2 furnizorilor externi de suport IT sau consultanților

2.2.3 tuturor angajaților responsabili pentru salvarea datelor în locații aprobate

3. Obiective

3.1 Să asigure că toate datele și sistemele critice ale organizației fac obiectul unui backup securizat, la intervale adecvate, în funcție de riscuri și de necesitățile operaționale.

3.2 Să asigure că datele pot fi recuperate complet și în timp util după întreruperi.

3.3 Să prevină accesul neautorizat, alterarea sau pierderea datelor de backup prin controale eficiente de stocare.

3.4 Să stabilească în mod clar rolurile și responsabilitățile pentru implementarea și testarea procedurilor de backup și să asigure respectarea acestora.

3.5 Să sprijine conformitatea cu ISO/IEC 27001, GDPR și alte obligații de reglementare prin practici de backup structurate și documentate.

4. Roluri și responsabilități

4.1 Director general (DG)

4.1.1 Aprobă prezenta politică și asigură aplicarea acesteia

4.1.2 Alocă resurse și desemnează responsabilități pentru activitățile de backup și restaurare

4.1.3 Revizuiește eșecurile de backup, incidentele sau abaterile de la politică

4.1.4 Coordonează revizuirea anuală a politicii și asigură pregătirea pentru audit

4.2 Furnizor extern de suport IT (dacă este cazul)

4.2.1 Implementează și administrează soluțiile de backup (locale sau în cloud)

4.2.2 Monitorizează execuția cu succes a backup-urilor și programează teste de restaurare

4.2.3 Raportează direct Directorului general eșecurile și incidentele

4.2.4 Asigură criptarea, restricțiile de acces și gestionarea corespunzătoare a mediilor de backup

[... 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 o dată pe an de către Directorul general. Situațiile care declanșează revizuiri intermediare includ:

9.1.1 schimbări majore ale sistemelor sau metodelor de stocare

9.1.2 introducerea unor noi platforme cloud sau soluții IT

9.1.3 modificări legislative sau de reglementare care afectează recuperarea datelor

9.1.4 constatări rezultate în urma auditurilor sau incidentelor

9.2 Directorul general este responsabil pentru inițierea revizuirii, aprobarea modificărilor și comunicarea actualizărilor.

9.3 Versiunile politicii trebuie urmărite și arhivate. Versiunile înlocuite trebuie să aibă acces restricționat pentru a evita confuziile în timpul auditurilor sau al activităților de recuperare a activității.

10. Politici conexe și interdependențe

10.1 Prezenta politică este aliniată cu și depinde de următoarele politici SME:

10.1.1 P14S – Politica de retenție a datelor și eliminare securizată: definește perioada de stocare a datelor de backup și modul în care acestea trebuie eliminate în mod securizat.

10.1.2 P13S – Politica de clasificare și etichetare a datelor: ajută la prioritizarea datelor care trebuie incluse în backup în funcție de nivelurile de clasificare.

10.1.3 P30S – Politica de răspuns la incidente: acoperă procedurile aplicabile dacă backup-urile eșuează sau dacă este necesară recuperarea datelor după o încălcare a securității sau o indisponibilitate.

10.1.4 P2S – Politica privind rolurile și responsabilitățile de guvernanță: atribuie autoritate clară pentru supravegherea backup-ului și aplicarea politicii.

10.1.5 P17S – Politica de protecție a datelor și confidențialitate: asigură că gestionarea backup-urilor care conțin date cu caracter personal este aliniată cu cerințele legale și de confidențialitate.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1: planificare și control operațional al sistemelor de backup ca parte a SMSI

11.2 ISO/IEC 27002

11.2.1 Controlul 8.13: stabilește bune practici pentru programarea, monitorizarea și restaurarea backup-urilor

11.2.2 Anexa A, controlul 5.29: integrarea backup-ului cu continuitatea activității și capacitatea de restaurare

11.3 NIST SP 800-53 Rev. 5

11.3.1 CP-9 (Planificarea continuității): definește strategii structurate de backup pentru reziliența organizației

11.3.2 MP-6 (Protecția mediilor): impune gestionarea și distrugerea securizată a mediilor de backup

11.4 GDPR al UE

11.4.1 Articolul 5 alineatul (1) litera (f): impune integritatea și disponibilitatea datelor cu caracter personal

11.4.2 Articolul 32 alineatul (1) litera (c): impune capacitatea de a restabili accesul la datele cu caracter personal în timp util

11.5 Directiva NIS2 a UE

11.5.1 Articolul 21 alineatul (2) litera (c): impune backup și recuperare ca parte a planificării rezilienței și continuității

11.6 Regulamentul DORA al UE

11.6.1 Articolul 10 alineatul (1): organizațiile din sectorul financiar trebuie să asigure backup-ul ca parte a măsurilor de continuitate TIC

11.7 COBIT 2019

11.7.1 BAI04.05: impune strategii de backup documentate

11.7.2 DSS04.07: subliniază testarea periodică și controlul proceselor de backup și recuperare a datelor