					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P15					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	Clauzele 6.1.3, 8	tratamentul riscurilor, planificare și controale operaționale pentru backup
ISO/IEC 27002:2022	Controalele 8.13, 5.28, 5.29	managementul backup-urilor, eliminare securizată și reziliență
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	cerințe privind backup-ul sistemelor, recuperarea și sanitizarea mediilor
GDPR al UE	Articolul 32, Considerentul 49	restaurarea și disponibilitatea datelor cu caracter personal, continuitatea activității
Directiva NIS2 a UE	Articolul 21(2)(c-e)	controale de backup și continuitate pentru reziliență
Regulamentul DORA al UE	Articolele 10, 11	cerințe privind backup-ul, recuperarea și testarea în sectorul financiar
COBIT 2019	DSS01, DSS04, MEA03	operațiuni de backup, continuitate și monitorizarea conformității

1. Scop

1.1 Scopul acestei politici este de a defini cerințele obligatorii pentru backup-ul și restaurarea datelor, sistemelor și aplicațiilor, în vederea susținerii rezilienței operaționale, integrității datelor și continuității activității.

1.2 Politica stabilește un cadru standardizat pentru:

1.2.1 protejarea datelor organizației împotriva pierderii cauzate de ștergere, corupere, defecțiuni sau atacuri cibernetice

1.2.2 definirea cerințelor de recuperare prin parametri clari RTO (Recovery Time Objective) și RPO (Recovery Point Objective)

1.2.3 integrarea operațiunilor de backup în cadrul mai larg al SMSI și în planurile de continuitate a activității și de recuperare în caz de dezastru (BCP/DRP)

1.2.4 asigurarea conformității cu legislația aplicabilă și cu reglementările sectoriale privind disponibilitatea și recuperabilitatea

1.3 Politica impune controalele ISO/IEC 27001:2022 referitoare la eliminarea securizată a datelor (5.28), reziliență (5.29) și backup-ul informațiilor (8.13) și este corelată cu bunele practici din ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, DORA și NIS2.

2. Domeniu de aplicare

2.1 Această politică se aplică:

2.1.1 tuturor sistemelor critice pentru activitatea organizației și sistemelor operaționale aflate în domeniul de aplicare al SMSI

2.1.2 tuturor datelor de business, structurate și nestructurate, inclusiv baze de date, fișiere, e-mailuri și configurații

2.1.3 tuturor mediilor — on-premises, cloud, hibride și stocare la distanță/în afara sediului

2.1.4 întregului personal responsabil pentru administrarea, executarea, verificarea sau restaurarea proceselor de backup

2.2 De asemenea, politica se aplică:

2.2.1 mediilor de backup și infrastructurii aferente, inclusiv benzi fizice, echipamente virtuale, instantanee de disc și soluții de backup în cloud

2.2.2 furnizorilor terți contractați pentru găzduirea, administrarea sau prelucrarea backup-urilor organizației

2.2.3 backup-ului jurnalelor, configurațiilor, pistelor de audit și documentației operaționale critice pentru continuitate

2.3 Sistemele excluse în mod explicit de la backup trebuie documentate, supuse unei evaluări a riscurilor și acceptate formal de Managerul SMSI și de proprietarul sistemului.

3. Obiective

3.1 Asigurarea faptului că toate sistemele și datele critice fac obiectul unui backup fiabil, cu o frecvență suficientă, redundanță adecvată și controale de securitate corespunzătoare.

3.2 Asigurarea unor mecanisme de restaurare care îndeplinesc cerințele definite privind RTO și RPO, în concordanță cu evaluările impactului asupra activității.

3.3 Menținerea unei documentații complete privind procedurile de backup, programele de retenție, rolurile și tehnologiile utilizate.

3.4 Validarea eficacității operațiunilor de backup prin teste sistematice de restaurare, jurnalizarea eșecurilor și urmărirea măsurilor de remediere.

3.5 Protejarea datelor de backup împotriva accesului neautorizat, modificării sau distrugerii pe întregul ciclu de viață al acestora.

3.6 Asigurarea conformității cu:

3.6.1 cerințele ISO/IEC 27001 privind controalele operaționale și de continuitate

3.6.2 familiile CP și MP din NIST SP 800-53 privind backup-ul și sanitizarea

3.6.3 Articolul 32 și Considerentul 49 din GDPR privind restaurarea accesului la date cu caracter personal

3.6.4 Articolul 10 din DORA și Articolul 21 din NIS2 privind continuitatea și reziliența TIC

3.7 Asigurarea faptului că serviciile de backup furnizate de terți respectă obligațiile contractuale și de reglementare în materie de securitate, inclusiv cerințele privind criptarea, eliminarea și protocoalele de notificare.

4. Roluri și responsabilități

4.1 Managementul executiv

4.1.1 aprobă această politică și se asigură că sistemele critice pentru activitatea organizației sunt protejate în mod adecvat prin practici aprobate de backup și restaurare

4.1.2 răspunde de asigurarea resurselor necesare operațiunilor de backup și de revizuirea periodică a acestora din perspectiva conformității cu reglementările

4.2 Directorul de securitate a informațiilor (CISO)

4.2.1 deține această politică și asigură alinierea cu cadrele mai largi de securitate a informațiilor, management al riscurilor și continuitate

4.2.2 supraveghează integrarea procedurilor de backup în BCP/DRP, răspunsul la incidente și planificarea rezilienței

4.2.3 revizuiește excepțiile de backup și evaluează propunerile de acceptare a riscului pentru excluderea sistemelor critice

[... 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 mai devreme, dacă revizuirea este declanșată de:

9.1.1 schimbări ale strategiei de continuitate a activității sau de recuperare în caz de dezastru

9.1.2 noi obligații legale sau de reglementare care afectează frecvența backup-urilor sau retenția datelor

9.1.3 schimbări în arhitectura sistemelor, instrumentele de backup sau furnizorii de servicii

9.1.4 incidente semnificative sau constatări de audit legate de pierderea datelor sau de eșecuri de recuperare

9.2 Revizuirea trebuie coordonată de CISO în colaborare cu:

9.2.1 echipa de infrastructură și operațiuni IT

9.2.2 Auditul intern

9.2.3 Responsabilul cu protecția datelor (DPO)

9.2.4 echipele de continuitate a activității și recuperare în caz de dezastru

9.3 Programele de backup, listele de includere a sistemelor, documentația de restaurare și registrele de excepții trebuie revizuite în paralel pentru a asigura:

9.3.1 acuratețea acoperirii backup-ului pentru toate activele critice

9.3.2 conformitatea cu cerințele privind RTO/RPO și retenția

9.3.3 caracterul complet al jurnalelor de testare și al rapoartelor de incident

9.3.4 remedierea deficiențelor de control identificate anterior

9.4 Toate actualizările trebuie:

9.4.1 să fie supuse controlului versiunilor și păstrate în depozitul de documente al SMSI

9.4.2 să includă un rezumat al modificărilor și justificarea acestora

9.4.3 să fie aprobate de managementul executiv

9.4.4 să fie comunicate întregului personal tehnic și de business afectat

10. Politici conexe și interdependențe

10.1 Această politică susține în mod direct și interacționează cu următoarele documente conexe:

10.1.1 P6 - Politica de management al riscurilor: identifică prioritizarea bazată pe risc a protecției prin backup pentru sisteme și servicii.

10.1.2 P12 - Politica de management al activelor: asigură că sistemele eligibile pentru backup sunt inventariate și corelate cu urmărirea ciclului de viață și clasificarea.

10.1.3 P13 - Politica de clasificare și etichetare a datelor: stabilește ce categorii de date necesită backup, inclusiv metadatele de etichetare necesare prioritizării.

10.1.4 P14 - Politica de păstrare și eliminare a datelor: corelează retenția backup-urilor cu limitele de retenție impuse de reglementări și cu eliminarea corespunzătoare a mediilor expirate.

10.1.5 P16 - Politica de mascare a datelor și pseudonimizare: susține minimizarea datelor în timpul backup-ului seturilor de date sensibile.

10.1.6 P30 - Politica de răspuns la incidente: se activează în cazul eșecurilor de backup, al problemelor de restaurare sau al compromiterii depozitelor de date de backup.

10.2 Aceste politici interconectate formează un cadru coerent, care asigură integrarea guvernanței backup-urilor în strategia mai largă a organizației privind SMSI și reziliența operațională.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001:

11.1.1 Clauza 6.1.3 - Plan de tratare a riscurilor: susține prioritizarea backup-urilor și planificarea restaurării pe bază de risc.

11.1.2 Clauza 8.1 - Planificare și control operațional: integrează controalele de recuperare și continuitate ca parte a măsurilor de protecție operaționale.

11.1.3 Controlul 5.28 din Anexa A - eliminare securizată sau reutilizare a echipamentelor: vizează sanitizarea securizată a mediilor de backup.

11.1.4 Controlul 5.29 din Anexa A - securitatea informațiilor în timpul perturbărilor: asigură capabilități de restaurare în timpul incidentelor sau dezastrelor.

11.1.5 Controlul 8.13 din Anexa A - backup-ul informațiilor: este abordat direct prin operațiuni de backup programate, testate și securizate.

11.2 ISO/IEC 27002:2022 - Controalele 8.13, 5.28, 5.29: aceste controale consolidează cerința privind backup-urile regulate, validarea integrității și planificarea restaurării în toate mediile IT.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - backup-ul sistemului: stabilește proceduri complete de backup, inclusiv stocarea în afara sediului și testarea restaurării.

11.3.2 CP-10 - recuperarea și restaurarea sistemului: impune proceduri validate pentru restaurare completă sau parțială, aliniate cu obiectivele de recuperare.

11.3.3 MP-6 - sanitizarea mediilor: asigură gestionarea securizată a mediilor de backup învechite.

11.3.4 SI-12 - proceduri de gestionare a informațiilor: consolidează responsabilitățile privind backup-ul și recuperarea datelor sensibile.

11.4 GDPR al UE (2016/679):

11.4.1 Articolul 32 - securitatea prelucrării: impune capabilități de restaurare și măsuri de protecție a disponibilității datelor, în special pentru datele cu caracter personal.

11.4.2 Considerentul 49: susține măsuri de continuitate a activității și recuperare în caz de dezastru, inclusiv backup-ul securizat ca parte a rezilienței organizației.

11.5 Directiva NIS2 a UE (2022/2555):

11.5.1 Articolul 21(2)(c-e): impune măsuri tehnice și organizatorice, inclusiv controale de backup și continuitate, pentru asigurarea rezilienței serviciilor.

11.6 DORA a UE (2022/2554):

11.6.1 Articolul 10 - continuitatea activității TIC: impune entităților financiare să dispună de backup complet al datelor, recuperare și planificarea continuității.

11.6.2 Articolul 11 - testarea planurilor de continuitate a activității TIC: subliniază validarea capabilității de recuperare prin testare periodică.

11.7 COBIT 2019:

11.7.1 DSS01 - operațiuni gestionate: susține furnizarea fiabilă a serviciilor prin protejarea disponibilității datelor.

11.7.2 DSS04 - continuitate gestionată: definește controale strategice și operaționale de continuitate, inclusiv backup-uri verificate.

11.7.3 MEA03 - monitorizarea, evaluarea și analizarea conformității: impune revizuirea periodică a măsurilor de continuitate, inclusiv a eficacității controalelor de backup.