					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P05					Titlul documentului: **Politica de management al schimbărilor**							
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, 5.15	Abordează acțiunile privind riscurile, controlul accesului și managementul schimbărilor
ISO/IEC 27002:2022	Controlul 8	Implementează un proces structurat de management al schimbărilor
NIST SP 800-53 Rev.5	CM-2 până la CM-14	Controale de management al configurației
GDPR UE	Articolele 32(1)(b–d), 25; Considerentul 78	Măsuri tehnice și organizatorice pentru securitatea sistemelor și a datelor pe durata schimbărilor
Directiva NIS2 a UE	Articolul 21(2)(a, b, d, e)	Impune managementul riscurilor asociate schimbărilor TIC
Regulamentul DORA al UE	Articolele 5, 8, 12	Reglementează riscul operațional/TIC și raportarea incidentelor
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Management structurat al schimbărilor IT, performanță, conformitate și cerințe

1. Scop

1.1. Prezenta politică stabilește un cadru formal pentru inițierea, evaluarea, aprobarea, implementarea și revizuirea schimbărilor aplicate sistemelor informatice, infrastructurii, aplicațiilor și proceselor conexe ale organizației.

1.2. Aceasta asigură executarea tuturor schimbărilor într-un mod controlat și verificabil, reducând la minimum riscul de întrerupere, compromitere a securității sau neconformitate cu reglementările.

1.3. Aceasta sprijină controlul 8.32 din Anexa A la ISO/IEC 27001:2022 prin impunerea unor practici de management al schimbărilor securizate, documentate și aliniate la risc.

1.4. Politica asigură, de asemenea, trasabilitatea deciziilor privind schimbările și promovează reziliența operațională pe durata modificărilor planificate sau de urgență.

2. Domeniu de aplicare

2.1. Prezenta politică se aplică tuturor schimbărilor care afectează sistemele, datele și mediile aflate în domeniul de aplicare al SMSI, inclusiv:

2.1.1. infrastructura IT (on-premises, cloud, medii hibride)

2.1.2. mediile de producție, preproducție și recuperare în caz de dezastru

2.1.3. aplicațiile de business, serviciile, API-urile și integrările

2.1.4. setările de configurare, aplicarea patch-urilor, lansările de software și migrările de sistem

2.1.5. remedierile de urgență și modificările planificate sau derulate în cadrul proiectelor

2.2. Aceasta reglementează schimbările inițiate de:

2.2.1. personal intern (operațiuni IT, dezvoltatori, proprietari de sistem)

2.2.2. furnizori externi, furnizori de servicii administrate (MSP) și contractori

2.2.3. echipe de proiect pe durata implementării sistemelor, upgrade-urilor sau tranzițiilor de servicii

2.3. Prezenta politică nu se aplică:

2.3.1. mediilor temporare de testare/dezvoltare fără acces la date de producție

2.3.2. configurațiilor personale ale utilizatorilor (acoperite de Politica de utilizare acceptabilă)

2.3.3. schimbărilor aduse sistemelor aflate în afara limitei de control a organizației, cu excepția cazului în care acestea afectează active integrate sau obligații prevăzute de politici

3. Obiective

3.1. Asigurarea faptului că toate schimbările sunt revizuite, aprobate, testate și documentate înainte de implementare.

3.2. Menținerea disponibilității sistemelor, integrității datelor și continuității serviciilor în timpul și după activitățile de schimbare.

3.3. Impunerea unor clasificări clare ale schimbărilor, a planificării revenirii și a evaluărilor de risc pentru toate tipurile de schimbări.

3.4. Facilitarea unui proces decizional transparent și a escaladării printr-o guvernanță structurată.

3.5. Sprijinirea pregătirii pentru audit prin înregistrări trasabile ale schimbărilor și revizuiri post-implementare.

3.6. Impunerea separării atribuțiilor și reducerea riscului de schimbări neautorizate sau conflictuale în sistemele critice.

4. Roluri și responsabilități

4.1. Managementul executiv

4.1.1. Aprobă Politica de management al schimbărilor și asigură alinierea acesteia la obiectivele strategice și obligațiile de reglementare.

4.1.2. Aprobă programele de schimbare cu impact ridicat sau transversale, ca parte a supravegherii de guvernanță.

4.1.3. Alocă resursele și bugetul necesare pentru instrumentele de control al schimbărilor și pentru instruirea personalului.

4.2. Comitetul consultativ pentru schimbări

4.2.1. Revizuiește și autorizează schimbările standard și majore, asigurând evaluarea adecvată a riscurilor, impactului și dependențelor.

4.2.2. Validează planurile de revenire, rezultatele testelor, comunicările către părțile interesate și programarea.

4.2.3. Este alcătuit din proprietari de sistem, reprezentanți ai securității informațiilor, ai operațiunilor IT, lideri de business și reprezentanți ai conformității.

4.2.4. Poate delega deciziile pentru schimbările cu risc scăzut sau pentru schimbările de urgență, în condiții documentate.

[... 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. Declanșatoare și frecvență de revizuire

9.1.1. Prezenta politică trebuie revizuită anual sau la apariția următoarelor situații:

9.1.1.1. schimbări majore în IT sau infrastructură

9.1.1.2. incidente semnificative legate de schimbări eșuate sau neautorizate

9.1.1.3. actualizări de reglementare sau noi obligații legale privind schimbările

9.1.1.4. implementarea unor noi instrumente sau platforme pentru sistemul de management al schimbărilor

9.2. Procesul de revizuire a Politicii de management al schimbărilor

9.2.1. Managerul de schimbare va coordona procesul de revizuire în colaborare cu:

9.2.1.1. IT, Securitate și Operațiuni

9.2.1.2. Audit intern și Managementul riscului

9.2.1.3. reprezentanții Comitetului consultativ pentru schimbări

9.2.2. Actualizările trebuie revizuite și aprobate de managementul executiv și de Comitetul de pilotaj al SMSI.

9.2.3. Versiunile republicate trebuie urmărite în Registrul documentelor și comunicate părților afectate, cu reconfirmare, după caz.

9.3. Controlul documentelor și versionare

9.3.1. Toate versiunile trebuie să includă:

9.3.1.1. ID-ul politicii, titlul și nivelul de clasificare

9.3.1.2. proprietarul și istoricul reviziilor

9.3.1.3. jurnalul schimbărilor și data intrării în vigoare

9.3.1.4. autoritatea de aprobare

9.3.2. Versiunile arhivate trebuie păstrate în conformitate cu Politica de păstrare a documentelor (minimum 3 ani).

10. Politici conexe și corelări

10.1. Prezenta politică este direct corelată cu și sprijină aplicarea următoarelor:

10.1.1. P1 – Politica de securitate a informației: stabilește cerința privind controale de securitate formale și responsabilitatea la nivel de proces, inclusiv guvernanța managementului schimbărilor.

10.1.2. P2 – Politica privind rolurile și responsabilitățile de guvernanță: definește autoritățile de aprobare și separarea atribuțiilor relevante pentru autorizarea și supravegherea schimbărilor.

10.1.3. P4 – Politica de control al accesului: asigură că permisiunile de acces pentru persoanele care implementează și revizuiesc schimbări respectă principiul privilegiului minim.

10.1.4. P6 – Politica de management al riscurilor: asigură că toate schimbările fac obiectul unei evaluări adecvate a riscului și al unor strategii de atenuare.

10.1.5. P33 – Politica de monitorizare a auditului și conformității: reglementează validarea și revizuirea de audit a înregistrărilor și încălcărilor legate de managementul schimbărilor.

10.2. Aceste politici permit, în mod colectiv, un ciclu de viață al managementului schimbărilor sustenabil, trasabil și securizat în cadrul SMSI.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001:2022

11.1.1. Clauza 6.1 – Acțiuni pentru abordarea riscurilor și oportunităților: prezenta politică sprijină identificarea, evaluarea și controlul riscurilor asociate schimbărilor.

11.1.2. Clauza 5.15 – Controlul accesului: asigură că accesul pe durata schimbărilor este controlat și trasabil.

11.1.3. Controlul 8.32 din Anexa A – Managementul schimbărilor: prezenta politică implementează integral cerința de a gestiona schimbările aduse facilităților și sistemelor de prelucrare a informațiilor într-un mod planificat și controlat.

11.2. ISO/IEC 27002:2022 – Controlul 8

11.2.1. Consolidează implementarea unui proces structurat de management al schimbărilor, incluzând clasificarea schimbărilor, aprobarea, testarea, revenirea și documentarea.

11.3. NIST SP 800-53 Rev.5

11.3.1. Familia CM (CM-1 până la CM-14): prezenta politică este strâns aliniată cu controalele de management al configurației, inclusiv configurațiile de bază de referință (CM-2), controlul schimbărilor de configurare (CM-3), analiza impactului asupra securității (CM-4) și restricțiile de acces (CM-5).

11.3.2. Familia AU (AU-2, AU-6, AU-12): mecanismele de jurnalizare și audit la care face referire această politică sprijină trasabilitatea evenimentelor și revizuirea conformității pentru activitățile legate de schimbare.

11.3.3. RA-3, RA-5: evaluările de risc determinate de schimbări și scanările de vulnerabilitate sunt integrate în procesul de evaluare a schimbărilor.

11.3.4. PM-11 (Definirea misiunii/procesului de business): asigură menținerea continuității activității și a obiectivelor operaționale pe durata schimbărilor.

11.4. GDPR UE (2016/679)

11.4.1. Articolul 32(1)(b–d): prezenta politică sprijină cerința privind măsuri tehnice și organizatorice adecvate pentru asigurarea securității datelor, în special pe durata schimbărilor de sistem.

11.4.2. Articolul 25 – Protecția datelor începând cu momentul conceperii și în mod implicit: asigură că schimbările care afectează datele cu caracter personal integrează confidențialitatea și securitatea în proiectare și implementare.

11.4.3. Considerentul 78: impune ca operatorii de date să implementeze mecanisme — cum ar fi politicile de control al schimbărilor — pentru a asigura în mod continuu confidențialitatea, integritatea și reziliența sistemelor de prelucrare.

11.5. Directiva NIS2 a UE (2022/2555)

11.5.1. Articolul 21(2)(a, b, d, e): impune măsuri tehnice și organizatorice pentru gestionarea riscurilor TIC, inclusiv a celor generate de schimbări de sistem, actualizări software și modificări de infrastructură.

11.6. Regulamentul DORA al UE (2022/2554)

11.6.1. Articolul 5 – Cadru de guvernanță și control intern: prezenta politică impune principii de management al riscului operațional corelate cu schimbările și actualizările TIC.

11.6.2. Articolul 8 – Cadru de management al riscurilor TIC: impune ca entitățile financiare să gestioneze toate schimbările care afectează sistemele TIC prin procese structurate de management al schimbărilor — reflectate în cerințele acestei politici privind clasificarea, testarea, revenirea și documentarea.

11.6.3. Articolul 12 – Raportarea incidentelor: asigură că schimbările eșuate care conduc la perturbări TIC sunt trasabile, documentate și raportate, după caz.

11.7. COBIT 2019

11.7.1. BAI06 – Schimbări IT gestionate: prezenta politică îndeplinește în mod direct obiectivele BAI06 prin stabilirea unor fluxuri structurate pentru aprobarea schimbărilor, evaluarea impactului, comunicare și testare.

11.7.2. BAI02 – Definirea gestionată a cerințelor și BAI03 – Identificarea și dezvoltarea gestionată a soluțiilor: asigură că schimbările determinate de nevoi de business sunt revizuite și implementate în condiții de securitate.

11.7.3. DSS01 – Operațiuni gestionate: sprijină integritatea continuă a sistemului pe durata implementării schimbărilor.

11.7.4. MEA01 și MEA03 – Monitorizare, evaluare și analiză a performanței și conformității: permit supravegherea continuă a eficacității și aplicării politicii de management al schimbărilor.