					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P05S					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**

Notă juridică (drepturi de autor și restricții de utilizare)

(C) 2025 Clarysec LLC. All rights reserved.

Acest document este proprietatea intelectuală a Clarysec LLC. Nicio parte a acestui document nu poate fi copiată, reutilizată, distribuită sau modificată în scopuri comerciale sau de implementare fără autorizare prealabilă expresă, în scris.

Utilizarea neautorizată este strict interzisă și poate conduce la acțiuni legale.

Pentru licențiere, contactați: info@clarysec.com

Aliniere la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 6.1, 8	
ISO/IEC 27002:2022	Controlul 8	
NIST SP 800-53 Rev. 5	CM-2 până la CM-5, CM-11	
Directiva UE NIS2	Articolul 21 alineatul (2) litera (b)	
Regulamentul UE DORA	Articolele 6 alineatul (9), 8 alineatul (4) litera (b)	
COBIT 2019	BAI06, DSS	

1. Scop

1.1 Această politică asigură că toate schimbările aduse sistemelor IT, configurațiilor, aplicațiilor de business sau serviciilor cloud sunt planificate, evaluate din perspectiva riscurilor, testate și aprobate înainte de implementare.

1.2 Scopul este reducerea întreruperilor operaționale, a riscurilor de securitate și a indisponibilității serviciilor, prin stabilirea unui proces simplificat, dar obligatoriu, aplicabil inclusiv întreprinderilor mici cu resurse limitate.

1.3 Această politică sprijină certificarea ISO/IEC 27001:2022 prin formalizarea modului în care sunt gestionate și documentate schimbările tehnice și operaționale.

2. Domeniu de aplicare

2.1 Această politică se aplică următoarelor categorii:

2.1.1 Angajaților și managerilor de departament care propun sau implementează schimbări

2.1.2 Furnizorilor externi de servicii IT care administrează sisteme sau aplicații software

2.1.3 Directorului general, care deține responsabilitatea generală pentru aprobarea schimbărilor

2.2 Aceasta acoperă schimbări privind:

2.2.1 Software-ul (actualizări, patch-uri, aplicații noi)

2.2.2 Hardware-ul (înlocuiri, modernizări)

2.2.3 Configurațiile de rețea și ale firewallurilor

2.2.4 Serviciile cloud, permisiunile de acces ale utilizatorilor sau integrările cu furnizori

2.2.5 Schimbările proceselor critice ale organizației care implică sisteme informatice

2.3 Atât schimbările planificate, cât și cele de urgență intră în domeniul de aplicare al acestei politici.

3. Obiective

3.1 Să asigure că toate schimbările aduse sistemelor IT și sistemelor organizației sunt autorizate, documentate și reversibile în cazul apariției unor probleme.

3.2 Să prevină perioadele de nefuncționare neplanificate, pierderea de date sau incidentele de securitate cauzate de schimbări necontrolate.

3.3 Să definească proceduri simple și repetabile pentru depunerea, aprobarea, testarea și revenirea în caz de eșec a schimbărilor.

3.4 Să mențină un registru al schimbărilor verificabil, care să susțină responsabilitatea operațională și conformitatea cu cerințele de reglementare.

3.5 Să permită luarea deciziilor pe baza riscului pentru schimbările semnificative sau sensibile.

4. Roluri și responsabilități

4.1 Directorul general

4.1.1 Deține responsabilitatea finală pentru toate schimbările majore.

4.1.2 Revizuiește și aprobă schimbările neobișnuite, critice sau cu risc ridicat.

4.1.3 Revizuiește registrul schimbărilor trimestrial sau după incidente majore.

4.2 Suportul IT sau furnizorul IT externalizat

4.2.1 Implementează schimbările, inclusiv actualizări de configurație, aplicarea patch-urilor și migrări de sisteme.

4.2.2 Menține un registru de bază al schimbărilor, care consemnează datele, tipurile de schimbare, rezultatele și persoanele care aprobă.

4.2.3 Testează schimbările înainte de implementare și aplică pașii de revenire, după caz.

4.2.4 Notifică utilizatorii afectați înainte și după schimbările majore.

[... 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 Revizuire anuală

9.1.1 Această politică trebuie revizuită anual de Directorul general sau de persoana de contact IT desemnată, pentru a asigura alinierea cu sistemele, fluxurile de lucru și cerințele de reglementare în vigoare.

9.2 Revizuiri intermediare

9.2.1 Revizuirile trebuie declanșate și în următoarele situații:

9.2.1.1 Incidente de securitate cauzate de gestionarea necorespunzătoare a schimbărilor

9.2.1.2 Introducerea unor sisteme IT noi

9.2.1.3 Modificări ale standardelor relevante, cum ar fi ISO, NIS2 sau DORA

9.3 Documentarea actualizărilor

9.3.1 Schimbările aduse acestei politici trebuie gestionate prin controlul versiunilor și aprobate de Directorul general. Fiecare versiune trebuie să consemneze data, rezumatul schimbărilor și aprobatorul.

9.4 Comunicarea politicii

9.4.1 Orice actualizări trebuie comunicate tuturor angajaților și furnizorilor externi afectați. Documentația trebuie actualizată în toate locațiile de referință (de exemplu, portalul personalului, unități partajate).

10. Politici conexe și corelări

10.1 Această politică este strâns corelată cu următoarele politici SME:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: Definește autoritatea de aprobare pentru schimbări.

10.1.2 P4S – Politica de control al accesului: Asigură că modificările de acces rezultate din schimbări sunt documentate și implementate corect.

10.1.3 P7S – Politica de integrare și încetare a raporturilor de muncă: Coordonează schimbările legate de tranzițiile de rol și alocarea accesului.

10.1.4 P15S – Politica de backup și restaurare: Asigură că pașii de revenire și recuperare pot fi executați dacă o schimbare eșuează.

10.1.5 P30S – Politica de răspuns la incidente: Reglementează modul în care schimbările eșuate sau neautorizate sunt tratate ca incidente de securitate.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 6.1 – Planificarea bazată pe risc trebuie să includă activitățile de schimbare.

11.1.2 Clauza 8.1 – Controalele operaționale trebuie aplicate în mod consecvent activităților legate de schimbare, pentru a asigura integritatea serviciilor.

11.2 ISO/IEC 27002

11.2.1 Controlul 8.32 – Oferă îndrumări pentru procese securizate de management al schimbărilor, inclusiv documentare, testare și aprobare.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Configurație de referință pentru sisteme înainte de schimbare.

11.3.2 CM-3 – Controlul schimbărilor de configurație.

11.3.3 CM-4 – Analiza impactului asupra securității.

11.3.4 CM-5 – Aprobarea și documentarea schimbărilor.

11.3.5 CM-11 – Auditul și monitorizarea schimbărilor.

11.4 Directiva UE NIS2

11.4.1 Articolul 21 alineatul (2) litera (b) – Impune proceduri formale pentru măsuri tehnice și organizatorice de securitate, inclusiv managementul schimbărilor.

11.5 Regulamentul UE DORA

11.5.1 Articolele 6 alineatul (9) și 8 alineatul (4) litera (b) – Impun entităților financiare să mențină procese de management al schimbărilor și al configurației pentru sistemele TIC.

11.6 COBIT 2019

11.6.1 BAI06 – Gestionarea schimbărilor: Evidențiază planificarea, evaluarea riscurilor și capacitatea de revenire.

11.6.2 DSS01 – Gestionarea operațiunilor: Asigură integritatea operațională în timpul tranzițiilor și schimbărilor tehnice.