					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P11					Titlul documentului: **Politica privind gestionarea conturilor de utilizator și a privilegiilor**							
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	Clauza 6.1.3, Clauza 8	-
ISO/IEC 27002:2022	Controalele 5.15-5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
GDPR al UE	Articolele 5(1)(f), 32; Considerentul 39	-
Directiva NIS2 a UE	Articolele 21(2)(a, d), 21(3)	-
Regulamentul DORA al UE	Articolele 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Scop

1 Prezenta politică stabilește controale obligatorii pentru gestionarea conturilor de utilizator și a privilegiilor în toate sistemele și serviciile informatice. Aceasta asigură că accesul la resursele organizației este acordat pe baza unei identități validate, a necesității determinate de rol și a principiilor privilegiului minim și separării atribuțiilor.

1.1 Aceasta susține angajamentul organizației față de securitatea informației prin implementarea unor procese structurate și verificabile pentru acordarea accesului, atribuirea privilegiilor, monitorizarea utilizării și revocarea conturilor.

1.2 Prezenta politică este esențială pentru reducerea riscului de acces neautorizat, utilizare abuzivă a privilegiilor, amenințări interne și neconformitate cu cadrele de reglementare aplicabile.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor angajaților, contractanților, furnizorilor terți de servicii, consultanților și altor persoane cărora li se acordă acces la resursele IT, aplicațiile sau datele organizației.

2.2 Aceasta reglementează toate sistemele și mediile în care sunt aplicate mecanisme de autentificare a utilizatorilor și control al accesului, inclusiv, fără a se limita la:

2.2.1 Aplicații corporative și baze de date

2.2.2 Platforme cloud și medii SaaS

2.2.3 Sisteme de operare și console administrative

2.2.4 Instrumente de acces la distanță și VPN-uri

2.2.5 Sisteme de management al identității și accesului

2.3 Politica include atât conturile standard de utilizator, cât și conturile privilegiate și cuprinde controale privind:

2.3.1 Crearea, modificarea și dezactivarea conturilor

2.3.2 Escaladarea privilegiilor la nivel de sistem și delegarea

2.3.3 Controlul și monitorizarea sesiunilor

2.3.4 Metodele de autentificare și gestionarea parolelor

3. Obiective

3.1 Să asigure că toate conturile de utilizator sunt identificabile în mod unic, autorizate corespunzător și alocate numai după validarea formală a necesității.

3.2 Să implementeze principiile privilegiului minim și să prevină accesul inutil sau excesiv prin aplicarea unor controale stricte asupra acordării și utilizării conturilor privilegiate.

3.3 Să impună actualizarea la timp a statutului conturilor în funcție de schimbările privind angajarea sau rolul, inclusiv dezactivarea imediată la încetarea activității.

3.4 Să permită detectarea și remedierea proactivă a conturilor inactive, utilizate abuziv sau neautorizate prin jurnalizare, revizuiri și automatizare.

3.5 Să mențină alinierea cu ISO/IEC 27001:2022 și standardele asociate și să îndeplinească obligațiile prevăzute de cadrele juridice și de reglementare relevante, precum GDPR, NIS2, DORA și COBIT 2019.

4. Roluri și responsabilități

4.1 Directorul de securitate a informațiilor (CISO)

4.1.1 Deține prezenta politică și asigură aplicarea acesteia la nivelul întregii organizații.

4.1.2 Revizuiește și aprobă orice excepții formale sau cazuri de acces de urgență.

4.1.3 Raportează constatările de audit legate de conturi și escaladează riscurile către managementul executiv.

4.2 Managerul controlului accesului / administratorul IT

4.2.1 Menține și operează controalele tehnice pentru gestionarea ciclului de viață al conturilor de utilizator.

4.2.2 Execută acțiuni de acordare a accesului, revocare a accesului și gestionare a privilegiilor pe baza unei solicitări aprobate.

4.2.3 Menține un registru de referință al tuturor conturilor de utilizator, al statutului acestora și al nivelului de privilegii.

4.2.4 Sprijină auditurile și revizuirile de conformitate prin furnizarea de jurnale și rapoarte de activitate.

[... 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 anual sau la apariția unor modificări semnificative privind:

9.1.1 Structura organizațională sau procesele de business

9.1.2 Sistemele IT, platformele de identitate sau metodele de acces

9.1.3 Cerințele de reglementare sau contractuale referitoare la managementul identității și accesului

9.2 Directorul de securitate a informațiilor (CISO), împreună cu Managerul controlului accesului, este responsabil pentru inițierea procesului de revizuire și coordonarea feedbackului din partea părților interesate.

9.3 Revizuirile intermediare pot fi declanșate de:

9.3.1 Incidente de securitate legate de utilizarea abuzivă a conturilor

9.3.2 Constatări de audit care evidențiază deficiențe în gestionarea ciclului de viață al conturilor

9.3.3 Implementarea unor noi instrumente de identitate sau de gestionare a accesului privilegiat (PAM)

9.4 Actualizările aduse prezentei politici trebuie să fie:

9.4.1 Supuse controlului versiunilor și înregistrate în biblioteca de documentație a SMSI

9.4.2 Comunicate tuturor părților interesate relevante, inclusiv șefilor de departament, operațiunilor IT și Resurselor Umane

9.4.3 Susținute de materiale de instruire și ghiduri procedurale actualizate

9.5 Toate modificările trebuie aprobate de managementul executiv sau de Comitetul de coordonare a securității informației și jurnalizate în scopuri de audit.

10. Politici conexe și corelări

10.1 Prezenta politică este corelată operațional și susținută de următoarele politici conexe din suita SMSI:

10.1.1 P4 Politica de control al accesului: stabilește principiile și mecanismele generale de control al accesului, inclusiv controale bazate pe reguli și controale bazate pe roluri.

10.1.2 P7 Politica de integrare și încetare a personalului: furnizează pașii procedurali pentru inițierea și încetarea accesului utilizatorilor, aliniați cu acțiunile HR.

10.1.3 P8 Politica privind conștientizarea și instruirea în domeniul securității informației: consolidează responsabilitățile utilizatorilor privind securitatea conturilor și protejarea credențialelor.

10.1.4 P13 Politica de clasificare și etichetare a datelor: orientează nivelurile de acces pe baza clasificării datelor, asigurând că limitele privilegiilor sunt aliniate cu nivelurile de sensibilitate.

10.1.5 P22 Politica de jurnalizare și monitorizare: asigură colectarea pistelor de audit pentru toate activitățile legate de conturi și revizuirea acestora pentru detectarea anomaliilor sau a utilizării neautorizate.

10.1.6 P30 Politica de răspuns la incidente: reglementează escaladarea, limitarea efectelor și acțiunile post-incident în cazurile de utilizare abuzivă a privilegiilor sau de activitate neautorizată a conturilor.

10.2 Fiecare dintre aceste politici funcționează împreună pentru a aplica un cadru coerent de management al identității și accesului, bazat pe risc, la nivelul întregii organizații.

11. Standarde și cadre de referință

11.1 Prezenta politică este aliniată cu standarde recunoscute la nivel global în domeniul securității cibernetice și cu cadre de reglementare care impun gestionarea securizată a identității, accesului și privilegiilor ca element esențial al securității informației în organizație.

11.2 ISO/IEC 27001:

11.2.1 Clauza 6.1.3 impune organizațiilor să determine, să evalueze și să trateze riscurile de securitate a informației, ceea ce face din gestionarea accesului și a privilegiilor un control formal, bazat pe risc, integrat în procesul de planificare al SMSI.

11.2.2 Clauza 8.1 - Planificare și control operațional: consolidează implementarea măsurilor tehnice și procedurale care reglementează accesul utilizatorilor și accesul privilegiat.

11.3 ISO/IEC 27002:2022 - Controalele 5.15 până la 5.18:

11.3.1 Controlul 5.15 - Managementul accesului utilizatorilor: susține procese formale pentru acordarea accesului, autorizarea accesului și revizuirea periodică a drepturilor de acces.

11.3.2 Controlul 5.16 - Managementul identității: stabilește unicitatea identității, controalele privind ciclul de viață și aplicarea autentificării securizate.

11.3.3 Controlul 5.17 asigură că acordarea și utilizarea drepturilor de acces sunt strict controlate, trasabile și aliniate cu principiul privilegiului minim pe tot parcursul ciclului de viață al contului de utilizator.

11.3.4 Controlul 5.18 - Drepturi de acces: este tratat integral prin atribuirea privilegiilor pe bază de rol, auditare și cerințe de aprobare pentru acces ridicat.

11.4 Aceste controale ghidează implementarea structurată a înregistrării și radierii conturilor, a separării privilegiilor și a utilizării informațiilor de autentificare. Politica impune guvernanța ciclului de viață al identității, acces just-in-time și monitorizarea sesiunilor privilegiate pentru a preveni utilizarea neautorizată a sistemelor.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Politica de control al accesului) și AC-2 (Managementul conturilor): reflectate prin cerințele politicii privind aprobarea accesului, maparea rolurilor și auditarea conturilor de utilizator.

11.5.2 AC-5 (Separarea atribuțiilor) și AC-6 (principiul privilegiului minim): îndeplinite prin restricționarea privilegiilor, alinierea la rolurile postului și dubla aprobare pentru activități cu risc ridicat.

11.5.3 IA-2 până la IA-5 (Identificare și autentificare): aplicate prin mecanisme puternice de autentificare, reguli privind ciclul de viață al credențialelor și cerințe de autentificare multifactor.

11.5.4 AU-2, AU-12 (Jurnalizare de audit și analiză): tratate prin înregistrarea sesiunilor și monitorizarea activităților privilegiate în mediile sensibile.

11.6 GDPR al UE (2016/679):

11.6.1 Articolul 32 - Securitatea prelucrării: impune controale de acces și mecanisme de verificare a identității pentru protejarea datelor cu caracter personal. Este îndeplinit prin impunerea aprobărilor de cont, a revizuirii privilegiilor și a măsurilor de autentificare puternică.

11.6.2 Articolul 5(1)(f) - Integritate și confidențialitate: asigură că datele cu caracter personal sunt accesate numai de utilizatori autorizați care au roluri legitime, aspect consolidat prin aplicarea controlului asupra gestionării conturilor.

11.6.3 Considerentul 39: solicită limitarea clară a accesului și asumarea răspunderii; prezenta politică susține trasabilitatea completă a identităților utilizatorilor și a atribuirilor de privilegii.

11.7 Directiva NIS2 a UE (2022/2555):

11.7.1 Articolul 21(2)(a, d): impune entităților să aplice politici de management al accesului și gestionarea securizată a credențialelor și a sesiunilor privilegiate, susținute prin controalele de alocare, monitorizare și excepții prevăzute în această politică.

11.7.2 Articolul 21(3): promovează disciplina accesului și un nivel ridicat de asigurare a identității în sectoarele critice, cerință îndeplinită prin utilizarea de identificatori unici, RBAC și acces ridicat restricționat în timp.

11.8 Regulamentul DORA al UE (2022/2554):

11.8.1 Articolul 5 - Guvernanță și control TIC: impune procese formalizate pentru gestionarea utilizatorilor TIC, acoperite prin acordarea accesului, dezactivare și tratarea excepțiilor, toate documentate.

11.8.2 Articolul 9 - Managementul riscurilor TIC: orientează organizațiile să securizeze sistemele prin restricții de acces și monitorizare, cerință adresată prin autentificare multifactor, jurnalizarea accesului privilegiat și revizuiri centralizate.

11.9 COBIT 2019:

11.9.1 DSS01 - Operațiuni gestionate: promovează aplicarea unor controale operaționale standardizate, inclusiv gestionarea ciclului de viață al conturilor de utilizator și documentarea accesului.

11.9.2 DSS05 - Servicii de securitate gestionate: reflectă administrarea securizată a privilegiilor utilizatorilor și sistemelor, susținând atenuarea riscurilor prin principiul privilegiului minim și validarea pistei de audit.

11.9.3 APO13 - Securitate gestionată: impune guvernanța accesului la activele digitale, cerință îndeplinită prin practici formalizate de autorizare a conturilor și rolurilor, completate de obligații de revizuire periodică.