					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P04S					Titlul documentului: **Politica de control al accesului**							
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 5	
ISO/IEC 27002:2022	Controalele 5.15, 5.16, 5	
NIST SP 800-53 Rev. 5	AC-1 până la AC-5	
GDPR	Articolul 32	
Directiva UE NIS2	Articolul 21(2)(b)	
Regulamentul UE DORA	Articolul 9	
COBIT 2019	APO07, DSS	

1. Scop

1.1. Prezenta politică definește modul în care organizația gestionează accesul la sisteme, date și facilități, pentru a se asigura că numai persoanele autorizate pot accesa informațiile pe baza necesității de serviciu.

1.2. Aceasta stabilește reguli clare pentru acordarea, modificarea, monitorizarea și revocarea accesului, pentru a reduce la minimum riscul de acces neautorizat și pentru a sprijini conformitatea cu legislația și standardele aplicabile.

1.3. Politica impune principiul privilegiului minim, astfel încât accesul să fie limitat la strictul necesar pentru îndeplinirea atribuțiilor de serviciu.

2. Domeniu de aplicare

2.1. Această politică se aplică tuturor persoanelor care utilizează sau gestionează accesul la sistemele IT, rețelele, datele sau facilitățile organizației, inclusiv:

2.1.1. Angajaților

2.1.2. Contractorilor

2.1.3. Lucrătorilor temporari

2.1.4. Furnizorilor externi de servicii IT

2.2. Aceasta acoperă accesul la:

2.2.1. Aplicațiile companiei, partajările de fișiere și bazele de date

2.2.2. Sistemele de e-mail, VPN și accesul la distanță

2.2.3. Serviciile cloud utilizate în scopuri de serviciu

2.2.4. Accesul fizic la facilități securizate, cum ar fi birouri sau camere de servere

2.3. Această politică se aplică tuturor dispozitivelor (emise de companie sau BYOD aprobat), platformelor și locațiilor.

3. Obiective

3.1. Să asigure că drepturile de acces sunt acordate numai în baza unei aprobări formale, pe baza rolului și a unei justificări de serviciu.

3.2. Să prevină accesul neautorizat sau excesiv la date sensibile, sisteme sau infrastructură.

3.3. Să definească proceduri clare pentru acordarea, modificarea și încetarea accesului utilizatorilor.

3.4. Să impună revizuirea periodică a drepturilor de acces și jurnalizarea automată sau manuală, pentru a sprijini auditurile.

3.5. Să sprijine aplicarea tehnică a restricțiilor de acces prin configurare și monitorizare.

4. Roluri și responsabilități

4.1. Directorul general

4.1.1. Aprobă prezenta politică și se asigură că sunt disponibile resursele necesare pentru implementarea unor controale de acces eficace.

4.1.2. Aprobă excepțiile și analizează auditurile anuale privind accesul.

4.2. Managerul IT / Furnizorul extern de servicii IT

4.2.1. Gestionează acordarea, modificarea și încetarea conturilor de utilizator.

4.2.2. Menține un Registru de control al accesului care cuprinde toate activitățile relevante (creări, modificări, eliminări).

4.2.3. Implementează controale de acces bazate pe roluri și impune autentificarea multifactor (de exemplu, MFA).

4.2.4. Revizuiește jurnalele de acces pentru a identifica activități suspecte și raportează problemele Directorului general.

[... 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. Revizuirea anuală a politicii

9.1.1. Managerul IT trebuie să revizuiască anual această politică. Orice schimbare în contextul juridic, tehnic sau organizațional trebuie să declanșeze o actualizare imediată.

9.2. Factori declanșatori ai revizuirii

9.2.1. Politica trebuie, de asemenea, revizuită dacă apare oricare dintre următoarele situații:

9.2.2. Schimbări majore de sistem sau migrări către cloud

9.2.3. Schimbări de roluri sau ale structurii organizaționale

9.2.4. Un incident de securitate a informațiilor care implică acces neautorizat

9.2.5. Schimbări de reglementare (de exemplu, actualizări ale GDPR, NIS2 sau DORA)

9.3. Documentarea și comunicarea schimbărilor

9.3.1. Revizuirile trebuie jurnalizate, cu istoricul versiunilor și aprobarea Directorului general, și comunicate întregului personal afectat.

9.4. Accesibilitate și instruire

9.4.1. Această politică trebuie pusă la dispoziția întregului personal, iar instruirea relevantă trebuie furnizată ca parte a procesului de integrare și ulterior, anual.

10. Politici conexe și corelări

10.1. Această politică trebuie aplicată în corelare cu următoarele politici SME, pentru asigurarea completă a practicilor de acces securizat:

10.1.1. P3S – Politica de utilizare acceptabilă: Asigură că utilizatorii înțeleg comportamentul acceptabil în raport cu accesul acordat.

10.1.2. P5S – Politica de management al schimbărilor: Asigură alinierea drepturilor de acces cu schimbările de sistem aprobate.

10.1.3. P7S – Politica de integrare și încetare a personalului: Definește punctele declanșatoare pentru acordarea accesului și pentru retragerea accesului utilizatorilor.

10.1.4. P17S – Politica de protecție a datelor și confidențialitate: Asigură alinierea controalelor de acces cu măsurile de protecție a datelor cu caracter personal.

10.1.5. P30S – Politica de răspuns la incidente: Definește modul în care incidentele legate de acces (de exemplu, utilizarea necorespunzătoare sau încălcările) sunt gestionate și investigate.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 5.15 – Impune politici și procese formalizate de control al accesului.

11.2. ISO/IEC 27002

11.2.1. Controalele 5.15–5.17 – Specifică orientări detaliate privind accesul bazat pe roluri, gestionarea ciclului de viață al accesului utilizatorilor și gestionarea accesului privilegiat.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 până la AC-5 – Impun politici structurate pentru managementul accesului, inclusiv autorizarea conturilor, revizuirea și monitorizarea.

11.4. GDPR

11.4.1. Articolul 32 – Impune controale tehnice și organizatorice (cum ar fi managementul accesului) pentru a asigura securitatea și confidențialitatea datelor.

11.5. Directiva UE NIS2

11.5.1. Articolul 21(2)(b) – Impune controale operaționale de acces și sisteme de management al identității pentru a preveni accesul neautorizat la sisteme.

11.6. Regulamentul UE DORA

11.6.1. Articolul 9 – Evidențiază necesitatea gestionării securizate a riscurilor TIC, inclusiv a unui control robust al accesului pentru entitățile financiare.

11.7. COBIT 2019

11.7.1. APO07 – Managed Security: prevede responsabilități privind accesul, definite și aplicate.

11.7.2. DSS01 – Manage Operations: include proceduri pentru gestionarea accesului logic și menținerea unor medii operaționale securizate.