					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P04					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	Clauzele 5.15, 5.17, 5.18	Managementul accesului logic și fizic
ISO/IEC 27002:2022	Controalele 8.2, 8.3	Acces bazat pe roluri și managementul identității
NIST SP 800-53 Rev. 5	AC-1 până la AC-20, IA-1 până la IA-8	Controale privind conturile/accesul, identitatea/autentificarea
GDPR	Articolele 5(1)(f), 32(1)(b); considerentul 39	Protecția datelor și minimizarea datelor
Directiva NIS2	Articolul 21(2)(c–e)	Controlul accesului, autentificarea utilizatorilor și protecția activelor
Regulamentul DORA	Articolele 6, 9(2)	Acces la TIC/al utilizatorilor și controale consolidate/terți
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Integrare, operațiuni, monitorizare, conformitate

1. Scop

1.1 Această politică stabilește principiile, responsabilitățile și cerințele obligatorii de control pentru gestionarea accesului la sistemele informatice, aplicații, facilități fizice și activele informaționale ale organizației.

1.2 Aceasta asigură că accesul este acordat pe baza nevoii de business, a rolului profesional și a profilului de risc, prin aplicarea unor principii precum privilegiul minim, necesitatea de a cunoaște și separarea atribuțiilor.

1.3 Politica sprijină implementarea clauzei 5.15 din ISO/IEC 27001:2022 și a controalelor conexe care reglementează accesul logic și fizic, autentificarea utilizatorilor și gestionarea ciclului de viață al accesului.

1.4 Această politică constituie baza pentru protejarea resurselor digitale și fizice împotriva utilizării neautorizate, utilizării abuzive sau compromiterii.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor utilizatorilor, sistemelor și facilităților aflate în domeniul de aplicare al SMSI, inclusiv:

2.1.1 angajaților, contractorilor, furnizorilor și personalului temporar

2.1.2 infrastructurii on-premises, sistemelor găzduite în cloud și mediilor hibride

2.1.3 tuturor activelor corporative — hardware, software, date și zone fizice securizate

2.1.4 accesului logic (de exemplu, sisteme, rețele, aplicații, API-uri) și accesului fizic (de exemplu, clădiri, centre de date)

2.2 Aceasta reglementează accesul pe întregul ciclu de viață al identității și al interacțiunii cu resursele, de la integrare și acordarea accesului până la schimbări de rol și încetarea colaborării.

2.3 Politica acoperă, de asemenea, contextul utilizării dispozitivelor personale în scop de serviciu (BYOD) și al accesului la distanță, asigurând consecvența controalelor indiferent de locație și de modelul de proprietate asupra dispozitivului.

3. Obiective

3.1 Să implementeze controale de acces securizate, bazate pe roluri, care să susțină integritatea operațională și conformitatea cu reglementările.

3.2 Să asigure că drepturile de acces sunt aprobate, monitorizate și revocate corespunzător și în timp util.

3.3 Să prevină accesul neautorizat, escaladarea privilegiilor sau menținerea unor drepturi de acces depășite.

3.4 Să sprijine principiile Zero Trust prin aplicarea implicită a refuzului accesului, cu excepția cazurilor aprobate și justificate în mod explicit.

3.5 Să ofere asigurare auditorilor și părților interesate prin revizuirea drepturilor de acces bazată pe dovezi și automatizată, precum și prin aplicarea consecventă a politicii.

3.6 Să integreze controlul accesului în procesele de business, evenimentele din ciclul de viață HR și arhitecturile tehnice.

4. Roluri și responsabilități

4.1 Managementul executiv

4.1.1 Aprobă Politica de control al accesului și asigură bugetul și resursele umane adecvate pentru aplicarea acesteia.

4.1.2 Revizuiește riscurile privind controlul accesului în cadrul analizei de management și alocă responsabilități la nivel strategic.

4.2 Directorul de securitate a informațiilor / responsabilul SMSI

4.2.1 Deține cadrul de control al accesului și asigură alinierea cu ISO/IEC 27001 și standardele conexe.

4.2.2 Coordonează aplicarea politicii, testarea și remedierea controalelor și raportarea indicatorilor privind controlul accesului.

4.2.3 Supraveghează modelarea accesului bazată pe risc și monitorizează deficiențele sistemice ale controalelor.

[... 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 pentru revizuire

9.1.1 Această politică trebuie revizuită:

9.1.1.1 anual, sau

9.1.1.2 în urma unei schimbări majore a infrastructurii IT, a cerințelor de reglementare sau a profilului de risc

9.1.1.3 după incidente care evidențiază deficiențe ale controalelor de acces

9.1.1.4 atunci când apar schimbări semnificative în tehnologiile de autentificare sau în platformele de identitate

9.2 Autoritatea și procesul de revizuire

9.2.1 Directorul de securitate a informațiilor sau responsabilul SMSI desemnat trebuie să gestioneze ciclul de revizuire, incluzând:

9.2.1.1 constatările auditului intern

9.2.1.2 rezultatele și indicatorii revizuirii accesului

9.2.1.3 actualizările juridice și de reglementare

9.2.1.4 schimbările platformelor tehnologice

9.2.2 Toate reviziile trebuie aprobate de managementul executiv și comunicate tuturor părților interesate.

9.2.3 Utilizatorilor afectați li se poate solicita să reconfirme luarea la cunoștință a politicii în urma unor actualizări semnificative.

9.3 Controlul versiunilor și documentația

9.3.1 Versiunea principală trebuie stocată în depozitul de documente al SMSI cu următoarele metadate:

9.3.1.1 numărul versiunii și jurnalul modificărilor

9.3.1.2 data intrării în vigoare și data următoarei revizuiri

9.3.1.3 proprietarul și autoritatea de aprobare

9.3.1.4 înregistrări privind distribuirea și luarea la cunoștință

9.3.2 Versiunile înlocuite trebuie arhivate și accesibile pentru o perioadă minimă de 3 ani.

10. Politici asociate și corelări

10.1 Această politică depinde funcțional de următoarele și trebuie interpretată împreună cu acestea:

10.1.1 P01 – Politica de securitate a informației: definește angajamentul organizației privind securitatea și așteptările de nivel înalt referitoare la controlul accesului.

10.1.2 P03 – Politica de utilizare acceptabilă: stabilește condițiile comportamentale pentru acces și responsabilitatea utilizatorilor privind utilizarea responsabilă a sistemelor.

10.1.3 P05 – Politica de management al schimbărilor: reglementează modul în care modificările configurațiilor de acces, ale rolurilor sau ale structurilor de grup trebuie implementate și testate în condiții de securitate.

10.1.4 P07 – Politica de integrare și încetare a personalului: determină inițierea și revocarea drepturilor de acces în conformitate cu evenimentele din ciclul de viață al utilizatorului.

10.1.5 P11 – Politica de gestionare a conturilor de utilizator și a privilegiilor: operaționalizează controalele la nivel de cont și completează această politică prin linii directoare tehnice pentru aplicarea accesului.

10.2 Împreună, aceste politici oferă un cadru coerent și aplicabil de guvernanță a accesului la nivelul unităților organizaționale și al tehnologiilor.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001:2022:

11.1.1 Clauza 5.15 – Controlul accesului: această politică îndeplinește cerința privind controlul accesului la informații și la alte active asociate, pe baza cerințelor de business și de securitate a informațiilor.

11.1.2 Clauza 5.17 – Managementul identității și Clauza 5.18 – Informații de autentificare: acestea sunt puse în aplicare prin provisionarea identităților, mecanismele de autentificare și atribuirea privilegiilor.

11.1.3 Controalele din anexa A 8.2 (Controlul accesului) și 8.3 (Managementul identității): furnizează baza pentru obiectivele de control ale acestei politici, inclusiv accesul bazat pe roluri, integrarea ciclului de viață al utilizatorului și protecția accesului privilegiat.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 Familia AC (AC-1 până la AC-20): această politică sprijină cerințele NIST privind controlul accesului atât pentru sistemele fizice, cât și pentru cele logice, inclusiv definirea politicii (AC-1), managementul conturilor (AC-2) și separarea atribuțiilor (AC-5).

11.2.2 Familia IA (IA-1 până la IA-8): oferă îndrumări pentru autentificarea identității, protecția credențialelor și MFA.

11.2.3 AU-2, AU-12: cerințele de jurnalizare și audit aplicate în baza acestei politici susțin responsabilizarea utilizatorilor și investigarea incidentelor.

11.2.4 PE-2 până la PE-6: tratează restricțiile de acces fizic, pe care această politică le aplică parțial prin controale cu badge-uri de acces în clădire și permisiuni de acces în clădiri.

11.3 GDPR (UE) 2016/679:

11.3.1 Articolul 5(1)(f): datele cu caracter personal trebuie protejate împotriva accesului neautorizat. Această politică asigură aplicarea tehnică și procedurală a acestui principiu.

11.3.2 Articolul 32(1)(b): impune implementarea controalelor de acces, a pseudonimizării și a criptării pentru prevenirea prelucrării neautorizate a datelor cu caracter personal.

11.3.3 Considerentul 39: impune minimizarea accesului la datele cu caracter personal, aplicată aici prin principiul privilegiului minim și cerințele de justificare a accesului.

11.4 Directiva NIS2 (UE) 2022/2555:

11.4.1 Articolul 21(2)(c–e): această politică permite măsuri tehnice și organizatorice pentru controlul accesului, autentificarea utilizatorilor și protecția activelor în cadrul entităților esențiale și importante.

11.5 Regulamentul DORA (UE) 2022/2554:

11.5.1 Articolul 6: impune politici de management al riscurilor TIC care includ explicit managementul accesului utilizatorilor și controale asupra ciclului de viață al identității. Această politică îndeplinește cerința respectivă pentru sectoarele financiar și al serviciilor TIC.

11.5.2 Articolul 9(2): această politică sprijină aplicarea unor controale puternice de acces ca parte a managementului serviciilor TIC prestate de terți și în interiorul grupului.

11.6 COBIT 2019:

11.6.1 APO07 – Gestionarea resurselor umane: aplică controale de integrare și încetare a colaborării pentru a susține guvernanța accesului.

11.6.2 BAI03 – Managed Solutions Identification and Build: integrează cerințele de control al accesului în proiectarea sistemelor și în procesele de schimbare.

11.6.3 DSS01 – Managed Operations și DSS05 – Managed Security Services: reglementează aplicarea restricțiilor de acces logic și monitorizarea încălcărilor.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: susține mecanismele de audit și asigurare pentru validarea eficacității controalelor de acces.