					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P07					Titlul documentului: **Politica de integrare și încetare a raporturilor de muncă sau de colaborare**							
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 7.2, Clauza 6	Competența personalului, integrarea securizată și aplicarea responsabilităților la încetarea sau schimbarea raporturilor de muncă ori de colaborare.
ISO/IEC 27002:2022	Controalele 6.2, 6.5, 5	Controale privind integrarea, accesul și ciclul de viață al personalului.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Tranziția și încetarea raporturilor cu personalul, principiul privilegiului minim, jurnalizarea de audit, managementul accesului în timpul și după modificările de personal.
GDPR al UE	Articolele 5(1)(f), 25, 32; Considerentul 39	Limitarea accesului, confidențialitate, protecție și controale adecvate pentru datele personalului.
Directiva NIS2 a UE	Articolul 21(2)(b, c, d)	Măsuri de securitate pentru personal și operațiuni; atenuarea amenințărilor interne; procese pe durata ciclului de viață.
Regulamentul DORA al UE	Articolele 5, 8, 9	Guvernanță, control intern TIC, risc TIC, managementul incidentelor în timpul tranziției personalului.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Resurse umane, managementul cunoștințelor, securitate și conformitate în procesele de integrare și încetare.

1. Scop

1.1 Prezenta politică stabilește proceduri standardizate pentru gestionarea integrării, a transferurilor interne și a încetării raporturilor de muncă sau de colaborare pentru toate categoriile de utilizatori.

1.2 Aceasta asigură alocarea și retragerea în timp util și în condiții de securitate a accesului fizic și logic, impunând totodată confidențialitatea, responsabilitatea și recuperarea activelor.

1.3 Această politică atenuează riscurile asociate accesului neautorizat, scurgerilor de date și activelor nereturnate prin integrarea controalelor de integrare și încetare în procesele de resurse umane, IT și securitate.

1.4 Aceasta sprijină Anexa A, Controlul 6.5 din ISO/IEC 27001:2022, asigurând aplicarea obligațiilor de securitate a personalului în timpul și după raportul de muncă sau de colaborare.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor angajaților, contractanților, consultanților, furnizorilor și altor terți cărora li se acordă acces la sistemele, rețelele, facilitățile sau datele organizației.

2.2 Aceasta reglementează întregul ciclu de viață al:

2.2.1 procesului de integrare (angajare, contractare sau colaborare temporară)

2.2.2 transferurilor interne sau schimbărilor de rol

2.2.3 încetării raporturilor de muncă sau de colaborare (demisie, pensionare, concediere, expirarea contractului)

2.3 Politica acoperă:

2.3.1 accesul logic (sisteme, aplicații, cloud, VPN)

2.3.2 accesul fizic (badge-uri, chei, sisteme de acces în clădire)

2.3.3 activele alocate (laptopuri, telefoane, tokenuri, credențiale)

2.3.4 confirmarea luării la cunoștință a politicilor și obligațiile de confidențialitate

2.4 Toate departamentele (Resurse umane, IT, Facilități, Securitate și Management) sunt responsabile pentru îndeplinirea rolului propriu în fluxurile de integrare și de încetare a raporturilor de muncă sau de colaborare.

3. Obiective

3.1 Să se asigure că întregul personal primește acces numai după îndeplinirea condițiilor prealabile privind securitatea, instruirea și cerințele contractuale.

3.2 Să se retragă drepturile de acces și să se recupereze activele organizației imediat după schimbarea rolului sau încetarea raporturilor de muncă ori de colaborare.

3.3 Să se păstreze confidențialitatea, integritatea și disponibilitatea (CIA) activelor organizației în timpul tranzițiilor de personal.

3.4 Să se sprijine trasabilitatea și susținerea juridică prin înregistrări complete ale evenimentelor de integrare și încetare.

3.5 Să se reducă expunerea la amenințări interne prin validarea și documentarea tuturor evenimentelor de acces asociate personalului.

3.6 Să se alinieze ciclul de viață al personalului din organizație cu practici de securitate bazate pe risc și cu cerințele de reglementare.

4. Roluri și responsabilități

4.1 Managementul executiv

4.1.1 Aprobă această politică și alocă autoritatea și resursele pentru procesele de integrare, încetare a raporturilor de muncă sau de colaborare și control al accesului.

4.1.2 Asigură că tranzițiile de personal nu expun organizația la riscuri de securitate sau juridice nejustificate.

4.2 Resurse umane

4.2.1 Inițiază fluxurile de integrare și încetare pentru angajați și notifică departamentele relevante cu privire la modificări.

4.2.2 Asigură finalizarea verificărilor antecedentelor, a contractelor, a acordurilor de confidențialitate (NDA) și a confirmării luării la cunoștință a politicii înainte de acordarea accesului.

4.2.3 Informează IT și departamentul de Facilități cu privire la plecările personalului, în conformitate cu SLA-ul de notificare.

4.2.4 Se coordonează cu departamentul juridic pentru aplicarea obligațiilor post-angajare (de exemplu, clauze de confidențialitate).

[... 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 Frecvența revizuirii politicii

9.1.1 Această politică trebuie revizuită:

9.1.1.1 anual, sau

9.1.1.2 după orice incident semnificativ care implică utilizarea abuzivă a accesului, pierderea de active sau un eșec procedural

9.1.1.3 la implementarea unor modificări majore ale platformelor HR sau IAM

9.1.1.4 la actualizări de reglementare sau juridice care afectează datele personalului ori obligațiile aferente

9.2 Procesul de revizuire și responsabilitatea

9.2.1 Managerul SMSI și Directorul de Resurse umane coordonează revizuirea, cu contribuții din partea securității IT, Juridicului și funcției de Conformitate.

9.2.2 Toate modificările trebuie aprobate de managementul executiv și de Comitetul de coordonare al SMSI.

9.2.3 Versiunile revizuite trebuie redistribuite departamentelor și persoanelor afectate pentru o nouă confirmare de luare la cunoștință.

9.3 Controlul documentelor și păstrarea

9.3.1 Această politică trebuie să includă:

9.3.2 controlul versiunilor, istoricul modificărilor și data intrării în vigoare

9.3.3 proprietarul responsabil și persoanele care efectuează revizuirea

9.3.4 clasificarea politicii și înregistrarea aprobării

9.3.5 Versiunile retrase trebuie arhivate pentru minimum 3 ani, în conformitate cu Politica de management al documentelor.

10. Politici conexe și corelări

10.1.1 Această politică se integrează direct cu:

10.1.2 P1 – Politica de securitate a informației: stabilește obiectivele de securitate ale organizației, inclusiv guvernanța accesului personalului.

10.1.3 P4 – Politica de control al accesului: stabilește cerințele operaționale pentru acordarea și retragerea accesului la sisteme și a accesului fizic pe baza declanșatoarelor de integrare și încetare.

10.1.4 P3 – Politica de utilizare acceptabilă: impune confirmarea luării la cunoștință în procesul de integrare și sprijină aplicarea cerințelor după încetare.

10.1.5 P6 – Politica de management al riscurilor: asigură evaluarea și atenuarea riscurilor legate de accesul utilizatorilor și de tranzițiile acestora, în conformitate cu principiile SMSI.

10.1.6 P11 – Politica privind conturile de utilizator și gestionarea privilegiilor: reglementează controalele tehnice pentru alocare și deprovizionare în sprijinul prezentei politici.

10.2 Aceste politici formează un sistem integrat de control pentru gestionarea în condiții de securitate și responsabilitate a evenimentelor din ciclul de viață al personalului.

11. Standarde și cadre de referință

11.1 Această politică este aliniată cu cadre recunoscute la nivel internațional în domeniul securității, protecției datelor și guvernanței IT, pentru a asigura că procesele de integrare și încetare sunt securizate, trasabile și conforme cu cerințele legale și organizaționale.

11.2 ISO/IEC 27001:

11.2.1 Clauza 7.2 – Competență și Clauza 6.2 – Obiective de securitate a informației: această politică sprijină dezvoltarea competenței personalului și integrarea în condiții de securitate a persoanelor în roluri care influențează obiectivele SMSI.

11.2.2 Anexa A, Controlul 6.5 – Responsabilități după încetarea sau schimbarea raportului de muncă: această politică aplică integral controalele privind drepturile de acces reziduale, custodia datelor și obligațiile contractuale la plecare.

11.2.3 Anexa A, Controlul 5.9 – Verificarea antecedentelor și 6.2 – Termeni și condiții de angajare: procedurile de integrare includ mecanisme de verificare a antecedentelor și de confirmare a politicilor, în concordanță cu aceste clauze.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Încetarea raporturilor cu personalul) și PS-5 (Transferul personalului): această politică impune eliminarea sau modificarea structurată a drepturilor de acces, a badge-urilor fizice și a activelor.

11.3.2 AC-2 (Managementul conturilor) și AC-6 (Principiul privilegiului minim): prevederile asigură alinierea accesului la rol și revocarea promptă atunci când acesta nu mai este necesar.

11.3.3 IA-4 (Managementul identificatorilor) și IA-5 (Managementul autentificatorilor): sprijină gestionarea securizată a credențialelor în timpul și după schimbările de personal.

11.3.4 CM-5 (Restricții de acces pentru schimbare): previne modificările neautorizate după încetare prin revocarea drepturilor de acces elevate.

11.3.5 AU-2 și AU-6: jurnalizarea și trasabilitatea evenimentelor de acces sunt consolidate prin integrarea IAM și a pistei de audit.

11.4 GDPR al UE (2016/679):

11.4.1 Articolul 5(1)(f): protejează datele cu caracter personal împotriva accesului neautorizat, cerință aplicată aici prin revocarea accesului utilizatorilor în procesul de încetare a raporturilor de muncă sau de colaborare.

11.4.2 Articolul 32: impune controale tehnice și organizaționale adecvate pentru securizarea datelor cu caracter personal pe durata ciclului de viață al raportului de muncă.

11.4.3 Articolul 25 – Protecția datelor începând cu momentul conceperii: asigură integrarea în procesele de integrare și încetare a minimizării datelor, retenției și controalelor privind accesul legal.

11.4.4 Considerentul 39: subliniază limitarea accesului și confidențialitatea, susținute prin structura prezentei politici.

11.5 Directiva NIS2 a UE (2022/2555):

11.5.1 Articolul 21(2)(b, c, d): impune măsuri de securitate pentru personal și operațiuni pentru a aborda controlul accesului, atenuarea amenințărilor interne și procesele pe durata ciclului de viață, toate reflectate în această politică.

11.6 Regulamentul DORA al UE (2022/2554):

11.6.1 Articolul 5 – Guvernanță și control intern: această politică sprijină guvernanța internă TIC aferentă riscului uman și managementului accesului.

11.6.2 Articolul 8 – Managementul riscurilor TIC: aplică controale tranzițiilor de personal care ar putea expune active critice sau medii reglementate.

11.6.3 Articolul 9 – Clasificarea și managementul incidentelor: asigură că încălcările legate de încetare sunt raportabile și atenuate prin deprovizionare și gestionarea activelor în mod corespunzător.

11.7 COBIT 2019:

11.7.1 APO07 – Gestionarea resurselor umane: definește rolurile, responsabilitățile și acțiunile din ciclul de viață pentru integrare și încetare, aliniate obiectivelor de guvernanță.

11.7.2 BAI08 – Managementul cunoștințelor: consolidează documentarea procedurilor, păstrarea cunoștințelor și transferul controalelor la sfârșitul raportului de muncă.

11.7.3 DSS05 – Servicii de securitate gestionate: impune dezactivarea utilizatorilor, controlul activelor și responsabilitatea în timpul tranzițiilor de rol.

11.7.4 MEA03 – Măsurare, evaluare și analiză a conformității: asigură evaluarea controalelor de integrare și încetare în cadrul auditurilor interne și externe.