					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P07S					Titlul documentului: **Politica de integrare și încetare a raporturilor de muncă ale personalului**							
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, după caz

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 6.2, 7	Cerințe privind securitatea resurselor umane și conștientizarea
ISO/IEC 27002:2022	Controalele 6.2, 6.5	Practici de securitate pentru integrarea și încetarea raporturilor de muncă
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Încetarea raporturilor de muncă; gestionarea ciclului de viață al conturilor; planificare
Directiva NIS2 a UE	Articolul 21(2)(h)	Securitatea resurselor umane și ciclul de viață al accesului
Regulamentul DORA al UE	Articolul 12	Controale de acces și revocare pentru sistemele TIC
COBIT 2019	APO07, DSS01	Securitatea personalului, controale de acces logic și fizic
GDPR al UE	Articolul 32	Securitatea datelor cu caracter personal pe durata raporturilor de muncă

1. Scop

1.1 Această politică definește procesul de integrare a noilor angajați sau contractori și de revocare securizată a accesului atunci când persoanele părăsesc organizația sau își schimbă rolul.

1.2 Aceasta asigură că accesul este acordat conform principiului privilegiului minim, că toate activele sunt evidențiate și că acțiunile critice, precum dezactivarea sistemelor și recuperarea datelor, sunt finalizate fără întârziere.

1.3 Această politică sprijină conformitatea, integritatea operațională și protecția datelor prin activități de integrare și încetare a raporturilor de muncă structurate și verificabile.

2. Domeniu de aplicare

2.1 Această politică se aplică:

2.1.1 tuturor angajaților permanenți și temporari

2.1.2 contractorilor, consultanților și stagiarilor

2.1.3 furnizorilor externi de servicii care au acces la sisteme sau acces fizic

2.2 Aceasta acoperă:

2.2.1 procesul de integrare: crearea conturilor de utilizator, acordarea accesului, alocarea echipamentelor

2.2.2 încetarea colaborării: eliminarea accesului, recuperarea activelor companiei și închiderea securizată a identităților digitale

2.2.3 schimbările interne de rol care necesită reconfigurarea accesului sau realocarea activelor

2.3 Se aplică tuturor dispozitivelor, platformelor și locațiilor utilizate în activitățile oficiale ale organizației.

3. Obiective

3.1 Să asigure că personalul nou primește acces și resurse pe baza rolurilor și responsabilităților verificate.

3.2 Să confirme că utilizatorii care părăsesc organizația sunt eliminați complet din sisteme și facilități până la sfârșitul ultimei lor zile de lucru.

3.3 Să prevină existența conturilor orfane și a activelor nereturnate, care prezintă un risc de securitate.

3.4 Să mențină înregistrări documentate ale acțiunilor de integrare, transfer și încetare a colaborării.

3.5 Să promoveze responsabilitatea prin liste de verificare și coordonarea rolurilor între funcții.

4. Roluri și responsabilități

4.1 Director general

4.1.1 Aprobă accesul pentru rolurile cu privilegii ridicate și supraveghează programul de integrare și încetare a raporturilor de muncă ale personalului.

4.1.2 Se asigură că excepțiile sunt justificate și că sunt întreprinse acțiuni corective atunci când procesele nu sunt respectate.

4.2 Office Manager / Resurse Umane

4.2.1 Inițiază procesul de integrare pentru noile angajări și notifică IT-ul cu privire la plecări.

4.2.2 Se asigură de finalizarea documentelor legale, de exemplu Acordul de confidențialitate (NDA), și a confirmărilor de luare la cunoștință a politicilor de securitate.

4.2.3 Menține listele de verificare pentru integrare și încetare și monitorizează conformitatea cu politica.

[... 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 cel puțin o dată pe an de către Directorul general și responsabilii HR/IT.

9.2 Declanșatori pentru revizuire anticipată

9.2.1 Actualizările trebuie efectuate dacă:

9.2.1.1 sunt introduse noi sisteme HR sau IT

9.2.1.2 se schimbă furnizorul extern de servicii IT sau serviciul externalizat de resurse umane

9.2.1.3 auditurile de securitate identifică lacune de proces

9.2.1.4 se modifică obligațiile de reglementare, de exemplu actualizări GDPR

9.2.1.5 are loc un eșec critic al procesului de încetare a colaborării sau o încălcare a securității

9.3 Controlul versiunilor și aprobare

9.3.1 Fiecare versiune a acestei politici trebuie să includă:

9.3.1.1 numărul versiunii și data

9.3.1.2 rezumatul modificărilor

9.3.1.3 aprobarea Directorului general

9.3.1.4 versiunile anterioare arhivate, păstrate cel puțin trei ani

9.4 Comunicare și luare la cunoștință

9.4.1 Tot personalul responsabil de integrare sau încetare trebuie notificat cu privire la orice actualizare a politicii. Sesiunile anuale de conștientizare sau instruirea anuală de reîmprospătare sunt obligatorii.

10. Politici conexe și corelări

10.1 Această politică susține și este susținută de următoarele:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: asigură responsabilitatea în procesele de acces și integrare

10.1.2 P4S – Politica de control al accesului: stabilește aplicarea tehnică a acordării accesului pe bază de roluri și a dezactivării

10.1.3 P6S – Politica de management al riscurilor: evaluează riscurile generate de deficiențele controalelor de integrare și încetare

10.1.4 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: impune cerințele de instruire introductivă a personalului în timpul integrării

10.1.5 P30S – Politica de răspuns la incidente: tratează neefectuarea deprovisionării accesului sau furtul de active ca incidente de securitate

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 6.2 – stabilește cerințele privind securitatea resurselor umane

11.1.2 Clauza 7.2 – impune instruirea de conștientizare pentru personalul nou

11.2 ISO/IEC 27002

11.2.1 Controalele 6.2 și 6.5 – detaliază practicile de securitate pentru integrarea și încetarea raporturilor de muncă

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – proceduri de încetare a raporturilor de muncă, inclusiv dezactivarea accesului

11.3.2 AC-2 – asigură gestionarea ciclului de viață al conturilor pentru accesul utilizatorilor

11.3.3 PL-4 – impune planificarea tranzițiilor de personal

11.4 GDPR al UE

11.4.1 Articolul 32 – asigură un nivel adecvat de securitate în timpul și după raporturile de muncă, în special pentru accesul la date cu caracter personal

11.5 Directiva NIS2 a UE

11.5.1 Articolul 21(2)(h) – impune controale privind securitatea resurselor umane și ciclul de viață al accesului

11.6 Regulamentul DORA al UE

11.6.1 Articolul 12 – impune entităților financiare reglementate să controleze accesul personalului la sistemele TIC, inclusiv procedurile de revocare

11.7 COBIT 2019

11.7.1 APO07 – Gestionarea resurselor umane: stabilește cerințele de securitate pentru ciclul de viață al personalului

11.7.2 DSS01 – Gestionarea operațiunilor: acoperă controlul accesului logic și fizic în timpul tranzițiilor de personal