					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P11S					Titlul documentului: **Politica privind conturile de utilizator și gestionarea 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	Clauzele 5.3, 8	Roluri, responsabilități și planificare/control operațional pentru gestionarea accesului utilizatorilor
ISO/IEC 27002:2022	Controlul 8	Controale pentru alocarea, revizuirea și retragerea privilegiilor ridicate
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Crearea conturilor, monitorizarea, principiul privilegiului minim și separarea atribuțiilor
GDPR al UE	Articolul 32	Controale de acces adecvate pentru protecția datelor cu caracter personal
Directiva NIS2 a UE	Articolul 21(2)(d)	Gestionarea accesului utilizatorilor pentru entitățile esențiale și importante
Regulamentul DORA al UE	Articolul 9(2)(b)	Controlul accesului privilegiat în entitățile financiare
COBIT 2019	DSS05.03, DSS05.04	Acordarea accesului, retragerea accesului și revizuirea periodică a accesului utilizatorilor

1. Scop

1.1 Prezenta politică stabilește reguli pentru gestionarea securizată, consecventă și trasabilă a conturilor de utilizator și a drepturilor de acces. Aceasta asigură că numai utilizatorii autorizați au acces la sisteme și date și că accesul este adecvat rolului și responsabilităților acestora.

1.2 Gestionarea eficace a conturilor și privilegiilor este esențială pentru prevenirea accesului neautorizat, reducerea amenințărilor interne și asigurarea conformității cu ISO/IEC 27001, GDPR și alte cerințe de reglementare aplicabile.

1.3 Această politică permite organizației să atribuie proprietatea și responsabilitatea pentru utilizarea conturilor, să monitorizeze și să auditeze elevarea privilegiilor și să dezactiveze sau să revoce în mod securizat accesul atunci când acesta nu mai este necesar.

1.4 De asemenea, aceasta protejează activitățile operaționale ale organizației împotriva erorilor operaționale sau a utilizării necorespunzătoare cauzate de acces excesiv ori nemonitorizat și contribuie la reducerea riscului de divulgare accidentală a informațiilor, utilizare abuzivă a privilegiilor sau neconformitate cu cerințele de reglementare.

2. Domeniu de aplicare

2.1 Această politică se aplică următoarelor:

2.1.1 tuturor angajaților, stagiarilor, contractorilor și utilizatorilor terți care au acces la sistemele IT ale organizației;

2.1.2 tuturor sistemelor, dispozitivelor, serviciilor și platformelor administrate de organizație sau în numele acesteia, inclusiv platformelor cloud, infrastructurii on-premises și instrumentelor terților.

2.2 Aceasta acoperă toate tipurile de conturi de utilizator, inclusiv:

2.2.1 conturi nominale de utilizator (de exemplu, conturi de e-mail, autentificări în sistem);

2.2.2 conturi de administrator și conturi la nivel de sistem;

2.2.3 credențiale de acces temporare, de tip guest sau pentru terți;

2.2.4 conturi de serviciu utilizate de aplicații sau sisteme de automatizare.

2.3 Politica se aplică pe întreg ciclul de viață al contului, de la creare și aprobare până la modificare, monitorizare și dezactivare. Aceasta include alocarea inițială a accesului în cadrul procesului de integrare, revizuirea drepturilor de acces în cazul schimbării rolului și revocarea în cadrul încetării colaborării.

3. Obiective

3.1 Atribuirea unor identități de utilizator unice și trasabile tuturor utilizatorilor de sistem, pentru a asigura responsabilizarea și a elimina dependența de credențiale partajate.

3.2 Aplicarea principiului privilegiului minim, astfel încât utilizatorilor să li se acorde numai nivelul minim de acces necesar pentru îndeplinirea atribuțiilor lor.

3.3 Prevenirea accesului neautorizat la sisteme sau date sensibile prin procese de aprobare și revizuire clar documentate.

3.4 Asigurarea dezactivării la timp a conturilor de utilizator atunci când acestea nu mai sunt necesare, de exemplu la încetarea raporturilor de muncă, finalizarea contractului sau schimbarea rolului.

3.5 Menținerea unui mediu documentat și verificabil prin documentarea tuturor modificărilor de cont, aprobărilor și revizuirilor periodice.

3.6 Asigurarea faptului că elevarea privilegiilor este strict controlată, aprobată independent și jurnalizată și că accesul ridicat este retras prompt atunci când nu mai este necesar.

4. Roluri și responsabilități

4.1 Director General

4.1.1 Are responsabilitatea generală pentru aplicarea prezentei politici.

4.1.2 Se asigură că practicile de gestionare a conturilor sunt aliniate la cerințele de certificare ISO/IEC 27001 și la obligațiile legale relevante (de exemplu, GDPR).

4.1.3 Trebuie informat imediat cu privire la orice acces neautorizat, incident de securitate a informațiilor sau încălcare a politicii legată de conturile de utilizator.

4.1.4 Asigură supravegherea revizuirilor politicii, a auditurilor și a măsurilor de aplicare.

4.2 Responsabil IT sau furnizor extern de servicii IT

4.2.1 Este responsabil pentru implementarea tehnică a controalelor privind conturile și privilegiile în toate sistemele utilizate de organizație.

4.2.2 Trebuie să efectueze acordarea accesului, modificarea și dezactivarea conturilor de utilizator exclusiv pe baza unor aprobări documentate.

4.2.3 Trebuie să aplice cerințele privind complexitatea parolelor, expirarea automată a sesiunii, autentificarea multifactor, dacă este disponibilă, și jurnalizarea sistemelor.

4.2.4 Trebuie să păstreze înregistrări securizate ale tuturor aprobărilor de acces, ale proprietății conturilor, ale escaladărilor de privilegii și ale revocărilor.

4.2.5 Are obligația de a monitoriza existența conturilor neautorizate sau a conturilor orfane și de a raporta neconcordanțele către Directorul 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 Prezenta politică trebuie revizuită cel puțin anual de Directorul General și de Responsabilul IT pentru a asigura conformitatea cu:

9.1.1 controalele și ghidurile curente ISO/IEC 27001:2022;

9.1.2 actualizările de reglementare (de exemplu, GDPR, DORA, NIS2);

9.1.3 modificările survenite în sisteme, servicii sau structura organizației.

9.2 Revizuirile trebuie efectuate, de asemenea, după:

9.2.1 incidente de securitate semnificative sau constatări de audit;

9.2.2 modificări majore ale sistemelor IT sau ale arhitecturii conturilor;

9.2.3 introducerea de noi platforme care necesită integrarea controlului accesului.

9.3 Toate modificările trebuie aprobate de Directorul General și comunicate clar personalului afectat.

10. Politici conexe și corelări

10.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: stabilește responsabilitatea și autoritatea decizională pentru aprobarea accesului și supraveghere.

10.2 P4S – Politica de control al accesului: reglementează aplicarea controlului accesului la nivelul întregului sistem și metodele de autentificare.

10.3 P7S – Politica de integrare și încetare a personalului: asigură includerea creării și eliminării conturilor în schimbările de personal administrate de Resurse Umane.

10.4 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: instruiește utilizatorii cu privire la practicile sigure de utilizare a conturilor și la așteptările privind utilizarea acestora.

10.5 P30S – Politica de răspuns la incidente: definește acțiunile care trebuie întreprinse dacă utilizarea abuzivă a conturilor conduce la un incident de securitate sau la o divulgare neautorizată.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 5.3: impune atribuirea clară și aplicarea rolurilor și responsabilităților pentru securitatea informațiilor.

11.1.2 Clauza 8.1: planificarea și controlul operațional trebuie să includă gestionarea accesului utilizatorilor.

11.2 ISO/IEC 27002

11.2.1 Controlul 8.2: detaliază controalele tehnice și procedurale pentru alocarea, revizuirea și retragerea privilegiilor ridicate.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: impune crearea conturilor, monitorizarea și revocarea pe baza unor roluri și procese definite.

11.3.2 AC-5: abordează separarea atribuțiilor pentru a preveni conflictele sau utilizarea abuzivă a privilegiilor.

11.3.3 AC-6: impune aplicarea principiului privilegiului minim tuturor drepturilor de acces.

11.4 GDPR al UE

11.4.1 Articolul 32: impune controale de acces adecvate pentru protejarea datelor cu caracter personal împotriva accesului neautorizat sau a alterării.

11.5 Directiva NIS2 a UE

11.5.1 Articolul 21(2)(d): impune gestionarea accesului utilizatorilor ca parte a controalelor de securitate de bază pentru entitățile esențiale și importante.

11.6 Regulamentul DORA al UE

11.6.1 Articolul 9(2)(b): impune entităților financiare să implementeze controale de acces care restricționează și monitorizează drepturile privilegiate.

11.7 COBIT 2019

11.7.1 DSS05.03: specifică acordarea accesului și retragerea accesului utilizatorilor ca parte a guvernanței IT.

11.7.2 DSS05.04: prevede revizuirea continuă și alinierea accesului utilizatorilor la rolurile din organizație.