					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P10S					Titlul documentului: **Politica privind biroul și ecranul curate**							
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 7.2, 8	
ISO/IEC 27002:2022	Controlul 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
Directiva UE NIS2	Articolul 21(2)(d)	
Regulamentul UE DORA	Articolul 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
GDPR	Articolul 32	

1. Scop

1.1 Această politică stabilește reguli obligatorii pentru menținerea unui mediu de lucru securizat, asigurând că birourile, stațiile de lucru și ecranele de afișare nu lasă la vedere informații confidențiale atunci când sunt nesupravegheate.

1.2 Scopul principal este prevenirea accesului neautorizat la informații sensibile prin documente tipărite lăsate nesupravegheate, ecrane neblocate sau medii de stocare amovibile pierdute, atât în mediile fizice de birou, cât și în locațiile de telemuncă.

1.3 Practicile privind biroul și ecranul curate definite în această politică consolidează capacitatea organizației noastre de a îndeplini cerințele de certificare ISO/IEC 27001 prin reducerea riscurilor de expunere care pot fi prevenite. Aceste practici oferă totodată clienților, partenerilor și auditorilor asigurarea că tratăm cu seriozitate securitatea informației, inclusiv în medii cu resurse limitate.

1.4 Această politică susține o cultură a responsabilității și a conștientizării, asigurând că întregul personal, indiferent de rol sau de nivelul de expertiză tehnică, înțelege responsabilitatea de a proteja informațiile companiei și ale clienților împotriva expunerii vizuale, furtului sau pierderii.

2. Domeniu de aplicare

2.1 Această politică se aplică:

2.1.1 tuturor angajaților, contractorilor, stagiarilor și lucrătorilor temporari care utilizează stații de lucru, birouri sau dispozitive mobile deținute de companie ori alocate individual

2.1.2 tuturor locațiilor fizice utilizate pentru activitățile organizației, inclusiv birouri dedicate, spații de coworking și spații de lucru la distanță/de la domiciliu

2.1.3 tuturor dispozitivelor digitale cu capabilități de afișare, inclusiv sisteme desktop, laptopuri, tablete și monitoare externe utilizate în scopuri profesionale

2.2 Politica se aplică oricărui activ fizic sau digital care poate afișa, conține sau transmite informații sensibile, inclusiv:

2.2.1 documentelor tipărite sau notițelor scrise de mână

2.2.2 unităților USB, CD-urilor și hard diskurilor externe

2.2.3 telefoanelor mobile utilizate pentru mesagerie de serviciu sau e-mail

2.2.4 monitoarelor și proiectoarelor conectate la sistemele de lucru

2.3 Această politică rămâne aplicabilă și în afara programului obișnuit de lucru, precum și în timpul activităților neobișnuite (de exemplu, mentenanță după program sau activități de răspuns în situații de urgență).

3. Obiective

3.1 Să impună controale practice și consecvente care să asigure că nicio informație sensibilă nu este lăsată expusă pe birouri, ecrane sau în spații comune.

3.2 Să reducă la minimum riscul de acces neautorizat, atât din surse interne (de exemplu, acces neintenționat de către alți angajați), cât și din amenințări externe (de exemplu, vizitatori, personal de curățenie sau contractori).

3.3 Să susțină restricțiile de acces fizic și logic prin impunerea obligației personalului de a securiza în mod activ materialele de lucru și de a bloca sistemele informatice atunci când acestea sunt lăsate nesupravegheate.

3.4 Să dezvolte gradul de conștientizare al personalului cu privire la practicile de lucru securizate și să stabilească reguli simple și obligatorii, aplicabile în activitățile de zi cu zi, indiferent de locul de desfășurare a activității.

3.5 Să asigure alinierea cu controlul 7.7 din Anexa A la ISO/IEC 27001 și cu ghidul de implementare corespunzător din ISO/IEC 27002 privind cerințele referitoare la biroul și ecranul curate.

3.6 Să asigure că organizația poate demonstra diligența necesară și pregătirea pentru audit fără a necesita infrastructură de nivel enterprise.

4. Roluri și responsabilități

4.1 Directorul general

4.1.1 Deține această politică și se asigură că este comunicată corespunzător, înțeleasă și respectată de toți angajații și contractorii.

4.1.2 Este responsabil pentru aprobarea oricăror excepții, gestionarea încălcărilor și supravegherea instruirii privind practicile de lucru securizate.

4.1.3 Trebuie să efectueze sau să delege verificări periodice (cel puțin trimestrial) pentru a confirma că spațiile de lucru fizice și digitale respectă cerințele politicii.

4.2 Membrul desemnat al personalului (dacă este numit)

4.2.1 I se poate atribui responsabilitatea pentru implementarea configurațiilor tehnice (de exemplu, setări de expirare a sesiunii și blocare a ecranului) sau pentru distribuirea mijloacelor fizice de stocare (de exemplu, sertare cu încuietoare).

4.2.2 Îl sprijină pe Directorul general prin raportarea neconformităților, transmiterea de reamintiri privind securitatea spațiului de lucru și urmărirea măsurilor de remediere atunci când sunt identificate probleme.

4.2.3 Contribuie la asigurarea faptului că toți angajații au acces, acolo unde este fezabil, la mecanisme de închidere adecvate sau la spații de stocare securizate.

[... 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 Directorul general trebuie să revizuiască această politică cel puțin o dată pe an și după oricare dintre următoarele evenimente:

9.1.1 introducerea unor noi spații de birouri, dispozitive sau sisteme partajate

9.1.2 modificări ale cerințelor legale sau de certificare aplicabile

9.1.3 constatări rezultate din audituri, evaluări de risc sau incidente de securitate

9.2 Actualizările intermediare trebuie comunicate tuturor angajaților prin e-mail, iar confirmarea de luare la cunoștință este obligatorie.

9.3 Versiunile anterioare ale acestei politici trebuie păstrate în condiții de securitate și într-o formă verificabilă, pentru a demonstra alinierea continuă la ISO/IEC 27001 și la cadrele aferente.

10. Politici conexe și corelări

10.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: clarifică autoritatea Directorului general de a aplica și audita comportamentul în spațiile de lucru fizice și digitale.

10.2 P4S – Politica de control al accesului: susține implementarea tehnică a blocării ecranului și a practicilor de autentificare securizată la stațiile de lucru.

10.3 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: consolidează instruirea comportamentală necesară pentru respectarea politicii.

10.4 P17S – Politica de protecție a datelor și confidențialității: definește obligațiile privind gestionarea și protejarea datelor cu caracter personal și a datelor sensibile în conformitate cu GDPR.

10.5 P30S – Politica de răspuns la incidente: stabilește cadrul de escaladare și răspuns în cazul în care o încălcare conduce la expunerea datelor sau la un incident de securitate a datelor.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 7.2: impune ca întregul personal să fie conștient de responsabilitățile de securitate, inclusiv de măsurile fizice de protecție.

11.1.2 Clauza 8.1: controalele operaționale trebuie să asigure măsuri de protecție fizice și logice adecvate.

11.2 ISO/IEC 27002

11.2.1 Controlul 7.7: oferă îndrumări detaliate privind stabilirea, comunicarea și aplicarea cerințelor referitoare la biroul și ecranul curate.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: stabilește cerințele privind controlul accesului fizic, inclusiv comportamentul personalului în medii securizate.

11.3.2 AC-11: impune funcționalitatea de blocare a sesiunii pentru stațiile de lucru, pentru a preveni vizualizarea sau interacțiunea neautorizată.

11.4 GDPR

11.4.1 Articolul 32: impune organizațiilor să protejeze datele cu caracter personal prin măsuri fizice și tehnice de protecție, inclusiv pentru stațiile de lucru și documente.

11.5 Directiva UE NIS2

11.5.1 Articolul 21(2)(d): impune organizațiilor să implementeze politici de acces fizic și logic bazate pe risc.

11.6 Regulamentul UE DORA

11.6.1 Articolul 9(2)(f): impune politici de securitate TIC, inclusiv practici de igienă a spațiului de lucru securizat, pentru operatorii din sectorul financiar și lanțurile lor de aprovizionare.

11.7 COBIT 2019

11.7.1 DSS01.06: impune practici de protecție a activelor, inclusiv controale fizice asupra spațiilor de lucru și mediilor de stocare.

11.7.2 DSS05.02: susține aplicarea practicilor de securitate pentru utilizatorii finali în toate mediile operaționale.