					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P10					Titlul documentului: **Politica privind biroul curat și ecranul securizat**							
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 6.1.3, Clauza 8	Plan de tratare a riscurilor, planificare și control operațional pentru spații de lucru securizate
ISO/IEC 27002:2022	Controlul 7	Controale comportamentale și de mediu pentru protejarea informațiilor fizice lăsate nesupravegheate
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Acces fizic, securitatea contractanților, eliminarea mediilor de stocare, blocarea sesiunii, controale de configurare și ale autentificatorilor
GDPR al UE	Articolele 5(1)(f), 32; Considerentul 39	Integritatea și confidențialitatea datelor, precum și măsuri fizice de protecție a datelor
Directiva NIS2 a UE	Articolele 21(2)(d), 21(3)	Politici privind securitatea fizică, comportamentul utilizatorilor și prevenirea scurgerilor de date
Regulamentul DORA al UE	Articolele 5, 8, 9	Guvernanță internă, TIC, managementul incidentelor care implică securitatea fizică
COBIT 2019	DSS01, DSS05, MEA	Operațiuni gestionate, servicii de securitate și monitorizarea conformității

1. Scop

1.1 Prezenta politică stabilește controale obligatorii pentru protejarea informațiilor sensibile, prin impunerea gestionării securizate a documentelor fizice, stațiilor de lucru, ecranelor și mediilor amovibile, atât în birouri, cât și în spații de lucru partajate.

1.2 Aceasta sprijină controlul 7.7 din Anexa A la ISO/IEC 27001 prin impunerea unor practici comportamentale și tehnice care reduc riscul de divulgare neautorizată, furt sau pierdere de date cauzate de informații lăsate nesupravegheate ori vizibile.

1.3 Prezenta politică consolidează securitatea fizică și securitatea informațiilor în activitățile zilnice și sprijină respectarea obligațiilor legale, contractuale și de reglementare aplicabile.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică întregului personal care își desfășoară activitatea în spații de lucru fizice sau le accesează, inclusiv:

2.1.1 angajaților permanenți și temporari

2.1.2 contractanților, consultanților, furnizorilor și stagiarilor

2.1.3 furnizorilor terți de servicii și vizitatorilor aflați la sediu care au acces la informații sensibile

2.2 Cerințele se aplică în:

2.2.1 birouri individuale, boxe de lucru și spații de lucru deschise

2.2.2 săli de ședință și zone comune de colaborare

2.2.3 zone de imprimare, recepții și camere pentru copiere

2.2.4 zone în care sunt utilizate stații de lucru la distanță sau terminale partajate

2.3 Prezenta politică se aplică, de asemenea, mediilor de lucru temporare sau hibride (de exemplu, hot-desking) și contextelor deschise publicului, în care există riscul observării ecranului de către alte persoane sau al lăsării datelor nesupravegheate.

3. Obiective

3.1 Prevenirea accesului neautorizat la informații confidențiale, sensibile sau reglementate lăsate expuse în format fizic sau digital.

3.2 Promovarea unui profil de risc standardizat la nivelul securității în toate mediile de lucru, prin utilizarea măsurilor fizice de protecție, a configurației stațiilor de lucru și a comportamentului utilizatorilor finali.

3.3 Reducerea riscului de încălcare a confidențialității, de pierdere a proprietății intelectuale și de exfiltrare a datelor cauzate de neglijență sau lipsă de atenție.

3.4 Integrarea comportamentului de birou curat și ecran securizat în cultura organizațională, pentru a susține disciplina operațională, trasabilitatea și capacitatea de a demonstra conformitatea în raport cu cerințele de reglementare.

3.5 Sprijinirea conformității cu ISO/IEC 27001, articolul 32 din GDPR, articolul 15 din NIS2 și alte cerințe relevante de securitate fizică pentru date critice sau cu caracter personal.

4. Roluri și responsabilități

4.1 Managementul executiv

4.1.1 Aprobă această politică și promovează o cultură orientată spre securitate în toate unitățile de business.

4.1.2 Alocă resurse adecvate pentru aplicarea politicii, campanii de conștientizare și mecanisme de control fizic.

4.2 Directorul de securitate a informațiilor / Managerul securității informațiilor

4.2.1 Este proprietarul acestei politici și asigură alinierea acesteia la ISO/IEC 27001:2022, cerințele de audit și strategiile de tratare a riscurilor.

4.2.2 Elaborează programe de conștientizare și controale pentru a asigura implementarea consecventă în toate spațiile și în mediile de lucru hibride.

4.2.3 Coordonează cu echipele administrative și IT pentru a asigura existența măsurilor fizice de protecție adecvate.

[... 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 Programul de revizuire a politicii

9.1.1 Prezenta politică trebuie revizuită:

9.1.1.1 cel puțin anual

9.1.1.2 după orice neconformitate de audit legată de expunerea spațiului de lucru sau a ecranului

9.1.1.3 în urma unui incident fizic sau de mediu (de exemplu, furt de dispozitive, acces neautorizat prin tailgating, supraveghere)

9.1.1.4 la implementarea unor noi configurații de birou, politici administrative sau modele de spațiu de lucru (de exemplu, hot-desking, hub-uri pentru lucru la distanță)

9.2 Proprietari responsabili

9.2.1 Proprietarul politicii este Directorul de securitate a informațiilor sau Managerul securității informațiilor desemnat.

9.2.2 Procesul de revizuire trebuie să implice:

9.2.2.1 echipele administrative și de securitate corporativă

9.2.2.2 IT și infrastructura pentru aplicarea cerințelor la nivelul dispozitivelor

9.2.2.3 Resurse Umane și Juridic pentru aplicarea cerințelor comportamentale și alinierea măsurilor disciplinare

9.2.3 Toate actualizările politicii trebuie gestionate prin controlul versiunilor, aprobate de Comitetul de coordonare al SMSI și redistribuite cu reluarea confirmării de luare la cunoștință, acolo unde este necesar.

9.3 Comunicarea modificărilor

9.3.1 Utilizatorii trebuie informați cu privire la actualizările semnificative prin:

9.3.1.1 centrul de politici din intranet sau portal

9.3.1.2 comunicări țintite prin e-mail

9.3.1.3 sesiuni de reîmprospătare la integrare și informări trimestriale

9.3.1.4 solicitări obligatorii de confirmare de luare la cunoștință pentru orice clauze noi critice privind aplicarea politicii

10. Politici conexe și corelări

10.1 Prezenta politică este aliniată cu și sprijină următoarele:

10.1.1 P1 – Politica de securitate a informației: stabilește așteptările privind comportamentul utilizatorilor și securitatea fizică, care stau la baza acestei politici.

10.1.2 P3 – Politica de utilizare acceptabilă: tratează responsabilitatea utilizatorilor pentru protejarea datelor și a sistemelor, inclusiv în mediile fizice.

10.1.3 P6 – Politica de management al riscurilor: include riscurile asociate spațiilor fizice de lucru ca parte a analizei riscurilor informaționale la nivelul întregii organizații.

10.1.4 P12 – Politica de management al activelor: sprijină urmărirea și gestionarea securizată a dispozitivelor și mediilor lăsate pe birouri.

10.1.5 P13 – Politica de clasificare și etichetare a datelor: stabilește legătura cu aplicarea cerințelor de birou curat pentru documentele fizice etichetate Confidențial sau Intern.

10.1.6 P14 – Politica de păstrare și eliminare a datelor: oferă îndrumări privind păstrarea documentelor fizice, distrugerea și gestionarea recipientelor de colectare.

10.1.7 P22 – Politica de jurnalizare și monitorizare: poate fi utilizată pentru monitorizarea stării de blocare a stațiilor de lucru, a timpului de inactivitate sau a fluxurilor video din spațiul de lucru, acolo unde este permis.

10.2 Aceste politici conexe stabilesc o cultură de securitate integrată, care combină conștientizarea utilizatorilor, măsurile fizice de protecție și asumarea responsabilității pentru a asigura spații de lucru reziliente.

11. Standarde și cadre de referință

11.1 Prezenta politică este aliniată cu standarde recunoscute la nivel global și cu cerințe legale care impun protejarea informațiilor sensibile în mediile fizice și prin comportamentul utilizatorilor.

11.2 ISO/IEC 27001

11.2.1 Clauza 6.1.3 – Plan de tratare a riscurilor: sprijină implementarea controalelor pentru reducerea riscurilor fizice și de mediu, inclusiv a celor asociate comportamentului utilizatorilor în spațiile de lucru deschise.

11.2.2 Clauza 8.1 – Planificare și control operațional: stabilește măsuri operaționale de protecție pentru gestionarea spațiilor de lucru securizate și a utilizării echipamentelor.

11.3 ISO/IEC 27002:2022 – Controlul 7

11.3.1 Acest control impune protecții comportamentale și de mediu pentru a preveni accesul neautorizat la informații prin intermediul mediilor, ecranelor sau materialelor tipărite lăsate nesupravegheate. Politica impune disciplina spațiului fizic de lucru, utilizarea blocării ecranului și eliminarea documentelor sensibile.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Autorizări de acces fizic): corelat prin restricțiile privind spațiul de lucru și impunerea stocării încuiate în mediile cu risc ridicat.

11.4.2 PS-7 (Securitatea personalului extern): aplicat prin extinderea cerințelor de birou curat și ecran securizat la contractanți și utilizatori terți.

11.4.3 MP-6 (Igienizarea mediilor de stocare) și AC-11 (Blocarea sesiunii): implementate prin proceduri de eliminare securizată și temporizatoare obligatorii de blocare a ecranului.

11.4.4 CM-6 (Setări de configurare) și IA-5 (Managementul autentificatorilor): susțin aplicarea tehnică a blocării ecranului și a controlului sesiunii pe echipamentele terminale.

11.5 GDPR al UE (2016/679)

11.5.1 Articolul 5(1)(f): impune integritatea și confidențialitatea datelor cu caracter personal, inclusiv protecția împotriva expunerii fizice sau a vizualizării de către persoane neautorizate.

11.5.2 Articolul 32 – Securitatea prelucrării: impune măsuri fizice și organizatorice adecvate pentru a proteja datele cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii sau divulgării neautorizate — realizate prin controale privind biroul și ecranul.

11.5.3 Considerentul 39: impune limitarea accesului la datele cu caracter personal la persoane autorizate — inclusiv prin securizarea acestora în format fizic atunci când sunt lăsate nesupravegheate.

11.6 Directiva NIS2 a UE (2022/2555)

11.6.1 Articolul 21(2)(d): impune politici și proceduri privind securitatea fizică și de mediu, inclusiv protecții ale securității informațiilor la nivelul spațiului de lucru.

11.6.2 Articolul 21(3): încurajează o cultură de securitate care include un comportament adecvat al utilizatorilor, conștientizare și prevenirea scurgerilor neintenționate de date — susținută prin controalele comportamentale din această politică.

11.7 Regulamentul DORA al UE (2022/2554)

11.7.1 Articolul 5 – Guvernanță și control intern: impune ca toate riscurile legate de TIC, inclusiv amenințările umane și de mediu, să fie guvernate prin politici aplicabile.

11.7.2 Articolul 8 – Managementul riscurilor TIC: impune măsuri de protecție atât în contexte digitale, cât și fizice, asigurând că utilizatorii la distanță, din sucursale și de la sediu nu creează expuneri negestionate.

11.7.3 Articolul 9 – Managementul incidentelor: impune ca abaterile de mediu sau comportamentale care conduc la expunerea datelor să fie jurnalizate, clasificate și tratate prin acțiuni corective adecvate.

11.8 COBIT 2019

11.8.1 DSS01 – Operațiuni gestionate: asigură disciplină operațională în protejarea spațiilor fizice de lucru și a sistemelor prin controale repetabile.

11.8.2 DSS05 – Servicii de securitate gestionate: sprijină protecția datelor, a dispozitivelor și a punctelor terminale de acces prin aplicarea unor cerințe bazate pe comportament, precum practicile de birou curat.

11.8.3 MEA03 – Monitorizarea, evaluarea și analizarea conformității: încurajează auditarea măsurilor fizice de protecție și a aplicării politicii în practicile zilnice ale organizației.