					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P09S					Titlul documentului: **Politica de telemuncă**							
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 standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controlul 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
Directiva UE NIS2	Articolele 21(2)(b), 21(2)(h)	NIS2 UE
Regulamentul UE DORA	Articolul 9	DORA UE
COBIT 2019	DSS05, APO13	COBIT 2019
GDPR UE	Articolul 32	GDPR UE

1. Scop

1.1 Prezenta politică stabilește cerințele de securitate pentru angajații și contractanții care lucrează la distanță, inclusiv de la domiciliu, din spații de lucru partajate sau în timpul deplasărilor.

1.2 Aceasta urmărește protejarea confidențialității, integrității și disponibilității (CIA) informațiilor de afaceri accesate în afara mediilor aflate sub controlul companiei.

1.3 Prezenta politică asigură conformitatea cu standardele internaționale și reduce riscurile precum accesul neautorizat, pierderea datelor și întreruperea serviciilor.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor membrilor personalului (angajați, contractanți, consultanți și lucrători temporari) care accesează sistemele, rețelele sau datele companiei în timp ce lucrează în afara sediului.

2.2 Aceasta acoperă:

2.2.1 Utilizarea dispozitivelor emise de companie și a dispozitivelor personale

2.2.2 Accesul prin VPN, desktop la distanță sau servicii cloud

2.2.3 Gestionarea securizată a informațiilor în afara sediilor companiei

2.2.4 Monitorizarea, gestionarea excepțiilor și aplicarea politicii

2.3 Aceasta se aplică atât regimurilor de telemuncă cu normă întreagă, cât și celor cu timp parțial, inclusiv accesului la distanță ad-hoc.

3. Obiective

3.1 Prevenirea accesului neautorizat la sistemele companiei sau la date sensibile în timpul telemuncii.

3.2 Asigurarea faptului că dispozitivele și legăturile de comunicații utilizate în afara biroului îndeplinesc cerințele minime de securitate.

3.3 Menținerea controlului asupra privilegiilor de acces la distanță și a activităților de monitorizare.

3.4 Furnizarea de îndrumări clare pentru angajați și manageri privind practicile de lucru securizat la distanță.

3.5 Respectarea cerințelor ISO, NIS2, GDPR, DORA și COBIT privind munca la distanță și mobilă.

4. Roluri și responsabilități

4.1 Director general

4.1.1 Aprobă regimurile de telemuncă și monitorizează conformitatea.

4.1.2 Escaladează incidentele de securitate sau cazurile repetate de nerespectare a cerințelor.

4.1.3 Revizuiește excepțiile și asigură urmărirea incidentelor.

4.2 Funcția IT sau furnizorul extern de servicii IT

4.2.1 Configurează în mod securizat accesul la distanță (de exemplu, VPN, gestionarea dispozitivelor mobile, autentificare multifactor).

4.2.2 Asigură aplicarea măsurilor de securitate pentru terminale, a criptării și a configurațiilor de securitate ale dispozitivelor.

4.2.3 Oferă suport utilizatorilor și investighează orice probleme tehnice de securitate.

[... 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 Revizuirea anuală a politicii

9.1.1 Directorul general și funcția IT trebuie să revizuiască anual prezenta politică pentru alinierea la schimbările tehnologice, de personal și legislative.

9.2 Declanșatoare pentru actualizare anticipată

9.2.1 Este necesară o revizuire imediată după:

9.2.1.1 Un incident major de securitate asociat telemuncii

9.2.1.2 Modificări ale cerințelor NIS2, GDPR sau DORA

9.2.1.3 Trecerea la o nouă tehnologie de acces la distanță (de exemplu, o platformă VPN diferită)

9.3 Controlul versiunilor și arhivarea

9.3.1 Toate versiunile prezentei politici trebuie să fie:

9.3.1.1 Datate și aprobate de Directorul general

9.3.1.2 Numerotate pe versiuni

9.3.1.3 Arhivate pentru o perioadă de cel puțin trei ani

9.4 Comunicarea către personal

9.4.1 Actualizările politicii trebuie comunicate tuturor utilizatorilor la distanță. Confirmarea luării la cunoștință este obligatorie pentru orice modificare semnificativă.

10. Politici conexe și corelări

10.1 Prezenta politică se corelează cu și susține următoarele:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: definește cine autorizează și supraveghează accesul la distanță

10.1.2 P4S – Politica de control al accesului: stabilește configurarea securizată a accesului la distanță și procedurile de revocare

10.1.3 P6S – Politica de management al riscurilor: urmărește și evaluează riscurile asociate accesului din afara sediului

10.1.4 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: instruiește utilizatorii cu privire la riscurile telemuncii și la bunele practici

10.1.5 P30S – Politica de răspuns la incidente: gestionează răspunsul la incidentele de acces la distanță, precum scurgerile de credențiale sau pierderea dispozitivelor

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 6.1 – Planificare bazată pe risc pentru scenarii de acces la distanță

11.1.2 Clauza 6.2 – Abordează responsabilitățile Resurselor umane în contexte mobile/la distanță

11.1.3 Clauza 8.1 – Planificare și control operațional al proceselor la distanță

11.2 ISO/IEC 27002

11.2.1 Controlul 6.7 – Oferă îndrumări practice privind securitatea pentru munca la distanță și mobilă

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Controlul accesului la distanță, protecția sesiunilor și monitorizarea securității

11.3.2 AC-2 – Controlul conturilor pentru utilizatorii din afara sediului

11.4 GDPR UE

11.4.1 Articolul 32 – Impune protecția datelor „prin proiectare și în mod implicit”, inclusiv în contexte la distanță

11.5 Directiva UE NIS2

11.5.1 Articolul 21(2)(b) – Impune utilizarea securizată a sistemelor informatice și de rețea

11.5.2 Articolul 21(2)(h) – Prevede măsuri de securitate asociate resurselor umane, inclusiv controale pentru activitatea desfășurată în afara sediului

11.6 Regulamentul UE DORA

11.6.1 Articolul 9 – Impune entităților financiare să mențină reziliența TIC în toate modurile operaționale, inclusiv pentru accesul la distanță

11.7 COBIT 2019

11.7.1 DSS05 – Manage Security Services: include securitatea terminalelor și practici securizate de lucru la distanță

11.7.2 APO13 – Managed Security: asigură implementarea securizată și supravegherea riscurilor pentru accesul mobil/la distanță