					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P09					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**

1. Scop

1.1 Această politică stabilește cerințele obligatorii pentru desfășurarea în condiții de securitate a telemuncii, inclusiv utilizarea sistemelor organizației, accesul la date și îndeplinirea atribuțiilor de serviciu în afara spațiilor corporative.

1.2 Aceasta asigură confidențialitatea, integritatea și disponibilitatea (CIA) activelor informaționale accesate de la distanță și stabilește controale pentru atenuarea riscurilor asociate mediilor de lucru distribuite.

1.3 Politica îndeplinește cerințele Anexei A, controlul 6.7 din ISO/IEC 27001:2022 prin implementarea de măsuri tehnice și procedurale adaptate condițiilor de lucru la distanță.

2. Domeniu de aplicare

2.1 Această politică se aplică întregului personal autorizat să lucreze de la distanță, inclusiv:

2.1.1 angajaților (cu normă întreagă, cu fracțiune de normă, contractuali)

2.1.2 furnizorilor externi de servicii IT, consultanților și altor furnizori

2.1.3 lucrătorilor temporari și personalului alocat pe proiecte care beneficiază de acces la distanță aprobat

2.2 Politica acoperă:

2.2.1 accesul la sistemele informatice ale organizației prin VPN sau prin instrumente de acces la distanță aprobate

2.2.2 gestionarea informațiilor sensibile și reglementate în afara spațiilor securizate

2.2.3 utilizarea echipamentelor deținute de organizație sau a dispozitivelor personale (BYOD)

2.2.4 măsurile de protecție fizică și logică din mediile de lucru la distanță

2.3 Politica se aplică în toate locațiile geografice și fusurile orare în care organizația permite telemunca, indiferent dacă aceasta este regulată, ad-hoc sau utilizată în cadrul evenimentelor de continuitate a activității.

3. Obiective

3.1 Să asigure că doar persoanele autorizate pot accesa de la distanță sistemele interne și informațiile.

3.2 Să impună criptarea, autentificarea multifactor și protecția punctelor terminale pe toate căile de acces la distanță.

3.3 Să mențină un profil de risc adecvat din perspectiva securității în raport cu amenințări precum atacurile de tip phishing, malware-ul, exfiltrarea datelor și expunerea neautorizată a sistemelor.

3.4 Să reglementeze modul în care datele sensibile sunt transmise, stocate sau tipărite în medii din afara sediului.

3.5 Să integreze măsuri de securitate fizică ce reduc vizibilitatea și observarea neautorizată în timpul sesiunilor la distanță.

3.6 Să asigure conformitatea cu cerințele internaționale de reglementare privind accesul la date de la distanță, inclusiv RGPD, NIS2 și DORA.

4. Roluri și responsabilități

4.1 Conducerea executivă

4.1.1 aprobă această politică și se asigură că sunt alocate resursele necesare și că aceasta este integrată în operațiunile de resurse umane, IT și securitate.

4.1.2 autorizează criteriile organizaționale de eligibilitate pentru telemuncă și aplicabilitatea acestora la nivelul unităților organizaționale.

4.2 Directorul de securitate a informațiilor / Managerul securității informației

4.2.1 deține și menține politica și se asigură de alinierea acesteia la profilul de risc și la cerințele de reglementare.

4.2.2 definește controalele de securitate pentru accesul la distanță (de exemplu, criptare, protecția punctelor terminale, expirarea sesiunilor).

4.2.3 aprobă gestionarea excepțiilor și monitorizează eficacitatea controalelor.

[... 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 Frecvența revizuirii

9.1.1 Această politică trebuie revizuită anual sau mai frecvent în cazul:

9.1.1.1 introducerii unor noi tehnologii de acces la distanță

9.1.1.2 extinderii semnificative a telemuncii (de exemplu, inițiative privind forța de muncă hibridă)

9.1.1.3 apariției unor noi amenințări, vulnerabilități sau incidente asociate mediilor la distanță

9.1.1.4 modificărilor cadrului juridic sau de reglementare relevant

9.2 Proprietate și procesul de revizuire

9.2.1 Proprietarul politicii este Directorul de securitate a informațiilor. Revizuirea trebuie coordonată cu:

9.2.1.1 operațiunile IT și arhitectura

9.2.1.2 resurse umane și facilități (pentru implicațiile operaționale și asupra spațiului de lucru)

9.2.1.3 responsabilul cu protecția datelor (pentru confidențialitate și controalele privind datele transfrontaliere)

9.2.2 Actualizările politicii trebuie:

9.2.2.1 să fie aprobate de Comitetul de coordonare al SMSI

9.2.2.2 să fie comunicate întregului personal afectat și contractanților

9.2.2.3 să fie integrate în materialele de instruire la angajare și de reîmprospătare

9.3 Controlul documentului și distribuirea

9.3.1 Politica trebuie să includă controlul versiunilor, data intrării în vigoare și istoricul modificărilor.

9.3.2 Versiunile înlocuite trebuie păstrate conform Politicii de management al documentelor (P14).

9.3.3 Versiunile revizuite trebuie să declanșeze o confirmare obligatorie de luare la cunoștință a politicii pentru utilizatorii eligibili pentru telemuncă.

10. Politici conexe și corelări

10.1 Această politică funcționează împreună cu:

10.1.1 P1 – Politica de securitate a informației: stabilește baza de referință pentru gestionarea securizată a activelor, aplicabilă tuturor mediilor de lucru, inclusiv celor la distanță.

10.1.2 P3 – Politica de utilizare acceptabilă: reglementează utilizarea adecvată a dispozitivelor și sistemelor organizației în timpul sesiunilor de telemuncă.

10.1.3 P4 – Politica de control al accesului: asigură faptul că privilegiile de acces la distanță respectă principiul privilegiului minim și mecanisme adecvate de autentificare.

10.1.4 P6 – Politica de management al riscurilor: definește modul în care riscurile asociate telemuncii sunt identificate, tratate și monitorizate în cadrul SMSI.

10.1.5 P12 – Politica de management al activelor: impune inventarierea și managementul configurației pentru toate dispozitivele utilizate de la distanță.

10.1.6 P22 – Politica de jurnalizare și monitorizare: asigură monitorizarea, auditarea și păstrarea sesiunilor la distanță conform cerințelor de conformitate.

10.1.7 P14 – Politica de păstrare și eliminare a datelor: definește regulile de gestionare a datelor relevante pentru telemuncă, inclusiv mediile amovibile și eliminarea securizată a dispozitivelor.

10.2 Aceste politici asigură în mod colectiv că telemunca este securizată, conformă și poate fi aplicată în toate funcțiile și în toate locațiile geografice.

11. Standarde și cadre de referință

11.1 Această politică este aliniată cu cadre recunoscute internațional privind securitatea, protecția datelor și managementul riscurilor TIC, pentru a asigura practici de telemuncă securizate, trasabile și conforme.

11.2 ISO/IEC 27001

11.2.1 Clauza 6.1.3 – Planificarea tratamentului riscului: această politică contribuie la tratarea riscurilor asociate accesului la distanță și mediilor de lucru distribuite.

11.2.2 Clauza 8.1 – Planificare și control operațional: impune implementarea de controale pentru sistemele accesate din afara spațiilor organizației.

11.2.3 Anexa A, controlul 6.7 – Lucrul la distanță: această politică acoperă integral controalele necesare pentru securitatea informației atunci când personalul lucrează în afara spațiilor organizației, inclusiv măsuri de protecție fizică și logică, guvernanța accesului și monitorizarea comportamentului utilizatorilor.

11.3 ISO/IEC 27002:2022 – Controlul 6

11.3.1 Acest control impune măsuri procedurale și tehnice pentru lucrul la distanță. Acesta include cerințe privind securitatea dispozitivelor, metodele de acces, gestionarea datelor, măsurile de protecție a mediului și managementul terților — toate fiind aplicate prin această politică.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Acces la distanță): susținut direct prin controale VPN, autentificare multifactor, jurnalizarea sesiunilor și autorizarea accesului bazată pe roluri pentru utilizatorii la distanță.

11.4.2 AC-2 (Managementul conturilor): controlează eligibilitatea accesului, atribuirea privilegiilor la distanță și dezactivarea conturilor.

11.4.3 SC-12 până la SC-13 (Protecție criptografică, stabilirea cheilor criptografice): implementate prin utilizarea obligatorie a VPN-urilor și a criptării complete a discului pentru punctele terminale la distanță.

11.4.4 MP-5 (Protecția transportului mediilor) și PE-18 (Localizarea componentelor sistemului informatic): ghidajul pentru telemuncă impune protecția transportului și măsuri de protecție fizică în mediile din afara sediului.

11.4.5 AU-2, AU-6: jurnalizarea și monitorizarea sesiunilor la distanță susțin cerințele de audit și răspuns la incidente.

11.5 RGPD al UE (2016/679)

11.5.1 Articolul 32 – Securitatea prelucrării: această politică aplică controale privind securitatea accesului la distanță, criptarea și jurnalizarea, necesare pentru protejarea datelor cu caracter personal accesate sau prelucrate de la distanță.

11.5.2 Articolul 5(1)(f): asigură că datele cu caracter personal accesate în afara sediului sunt protejate împotriva prelucrării neautorizate sau ilegale și a pierderii accidentale.

11.5.3 Considerentul 39: evidențiază limitarea accesului, integritatea și confidențialitatea — aspecte deosebit de relevante atunci când dispozitivele părăsesc spațiile securizate.

11.6 Directiva NIS2 a UE (2022/2555)

11.6.1 Articolul 21(2)(a, b, d): impune securizarea accesului la distanță ca parte a cadrului de management al riscurilor TIC al organizației. Această politică îndeplinește cerința privind măsurile de securitate care acoperă controlul accesului, securitatea datelor și politicile organizaționale pentru mediile la distanță.

11.6.2 Articolul 21(3): încurajează conștientizarea în domeniul securității și aplicarea politicii în rândul personalului care lucrează în afara spațiilor centrale.

11.7 Regulamentul DORA al UE (2022/2554)

11.7.1 Articolul 5 – guvernanță și cadru de control intern: această politică susține așteptările privind controlul riscurilor TIC pentru toate scenariile operaționale, inclusiv modelele hibride și la distanță.

11.7.2 Articolul 8 – cadrul de management al riscurilor TIC: riscurile asociate accesului la distanță sunt identificate, atenuate și guvernate prin controale tehnice și organizaționale aplicate prin prezenta politică.

11.7.3 Articolul 9 – mecanisme de partajare a informațiilor: protejează împotriva divulgării la distanță a informațiilor partajate în cadrul rețelelor de reziliență operațională digitală.

11.8 COBIT 2019

11.8.1 DSS01 – operațiuni gestionate: această politică susține continuitatea securizată a activităților operaționale ale organizației, indiferent de locația fizică.

11.8.2 BAI06 – schimbări IT gestionate și BAI09 – active gestionate: asigură că dispozitivele utilizate pentru telemuncă sunt urmărite, configurate securizat și tratate ca active critice.

11.8.3 APO13 – securitate gestionată: promovează un cadru definit de guvernanță a securității pentru mediile la distanță.

11.8.4 MEA03 – monitorizarea, evaluarea și analiza conformității: stabilește că activitatea de telemuncă trebuie jurnalizată, revizuită și auditată.