					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P34S					Titlul documentului: **Politica privind dispozitivele mobile și utilizarea dispozitivelor proprii (BYOD)**							
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**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 5.1, 5.2, 6.1, 6.2, 8	Cerințe generale privind Sistemul de Management al Securității Informației (SMSI) și controalele pentru dispozitive mobile/BYOD
ISO/IEC 27002:2022	Controalele 5.10–5.13	Controale detaliate pentru dispozitive mobile/BYOD și acces la distanță
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Controale federale privind dispozitivele, mediile de stocare și configurarea
GDPR al UE	Articolul 5(1)(f)	Protecția datelor cu caracter personal/protecția terminalelor mobile
Directiva NIS2 a UE	Articolul 21(2)(d)	Protecția dispozitivelor critice pentru activitățile organizației (inclusiv BYOD)
Regulamentul DORA al UE	Articolele 9, 10	Managementul riscurilor TIC/continuitatea pentru terminalele mobile
COBIT 2019	APO13, DSS01, DSS05	Guvernanță IT, operațiuni și controale pentru serviciile de securitate

1. Scop

1.1. Această politică stabilește cerințele de securitate obligatorii pentru utilizarea dispozitivelor mobile — inclusiv smartphone-uri, tablete și laptopuri — la accesarea informațiilor, sistemelor sau serviciilor companiei.

1.2. De asemenea, aceasta reglementează utilizarea dispozitivelor proprii (BYOD), pentru a asigura protecția datelor clienților și a datelor organizației, indiferent de proprietarul dispozitivului.

1.3. Politica impune măsuri de protecție consecvente pentru accesul mobil, sprijină îndeplinirea obiectivelor de certificare ISO/IEC 27001 și previne pierderea sau compromiterea datelor ca urmare a pierderii, furtului sau utilizării necorespunzătoare a terminalelor mobile.

1.4. Aceasta asigură aplicarea măsurilor tehnice și procedurale de protecție pentru utilizarea mobilă în IMM-uri fără echipe IT dedicate, inclusiv în medii de lucru la distanță și în servicii cloud.

2. Domeniu de aplicare

2.1. Această politică se aplică tuturor angajaților, contractorilor, stagiarilor și furnizorilor de servicii care:

2.1.1. Utilizează un dispozitiv mobil pentru a accesa, prelucra sau stoca date sau sisteme ale companiei

2.1.2. Se conectează la serviciile companiei, inclusiv e-mail, foldere partajate, aplicații cloud sau sisteme interne prin VPN

2.2. Politica acoperă:

2.2.1. Toate dispozitivele mobile: smartphone-uri, tablete, laptopuri (furnizate de companie sau dispozitive personale BYOD)

2.2.2. Toate sistemele de operare (de exemplu, iOS, Android, Windows, macOS)

2.2.3. Toate locațiile (birou, domiciliu, la distanță, spații publice)

2.3. Politica se aplică în toate mediile de lucru și trebuie respectată indiferent de proprietarul dispozitivului.

3. Obiective

3.1. Prevenirea pierderii datelor: Asigurarea faptului că utilizarea dispozitivelor mobile nu expune date sensibile ale companiei sau ale clienților la acces neautorizat, furt sau utilizare abuzivă.

3.2. Stabilirea unor reguli clare pentru BYOD: Definirea unor condiții aplicabile și obligatorii pentru utilizarea dispozitivelor personale în scop de serviciu, cu asigurarea măsurilor de protecție juridice și tehnice.

3.3. Sprijinirea conformității cu reglementările: Îndeplinirea cerințelor ISO/IEC 27001, GDPR, NIS2 și a altor obligații legale prin practici obligatorii de securitate mobilă.

3.4. Reducerea riscului operațional: Reducerea probabilității unor perturbări operaționale cauzate de utilizarea necorespunzătoare, compromiterea sau defectarea dispozitivelor mobile.

3.5. Menținerea încrederii clienților: Demonstrarea către clienți și parteneri a faptului că datele lor rămân protejate chiar și atunci când sunt accesate de pe dispozitive mobile sau personale.

4. Roluri și responsabilități

4.1. Director general (GM):

4.1.1. Păstrează responsabilitatea generală pentru această politică.

4.1.2. Aprobă orice utilizare a accesului mobil și a BYOD la sistemele companiei.

4.1.3. Se asigură că acordurile BYOD sunt semnate, păstrate și monitorizate.

4.1.4. Verifică faptul că furnizorii externi de servicii IT aplică măsurile de protecție necesare pentru utilizarea dispozitivelor mobile.

4.2. Personal desemnat sau suport IT:

4.2.1. Oferă asistență pentru configurarea, înregistrarea și setarea dispozitivelor mobile utilizate în scop de serviciu.

4.2.2. Aplică controalele de acces aferente utilizării dispozitivelor mobile, restricțiile privind aplicațiile și politicile de monitorizare.

4.2.3. Sprijină răspunsul la incidente care implică dispozitive mobile (dispozitive pierdute, furate sau compromise).

[... 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. Revizuire anuală

9.1.1. Directorul general (GM) trebuie să revizuiască această politică cel puțin o dată la 12 luni.

9.1.2. Revizuirea trebuie să verifice menținerea alinierii cu cerințele ISO/IEC 27001, evoluția tehnologiilor mobile și schimbările din activitățile organizației.

9.1.3. Actualizările trebuie, de asemenea, să țină seama de incidentele recente, rezultatele auditului sau evoluțiile de reglementare (de exemplu, GDPR, NIS2, DORA).

9.2. Evenimente declanșatoare pentru revizuirea intermediară

9.2.1. Această politică trebuie actualizată imediat dacă intervine oricare dintre următoarele situații:

9.2.1.1. Un incident major de securitate mobilă (de exemplu, o breșă de securitate cauzată de un dispozitiv pierdut sau compromis prin atac informatic)

9.2.1.2. O schimbare a platformelor suportate sau a instrumentelor de management al dispozitivelor mobile

9.2.1.3. O schimbare legislativă sau de reglementare care afectează utilizarea dispozitivelor personale sau protecția datelor

9.2.1.4. Introducerea unor noi aplicații, servicii sau instrumente terțe utilizate pe dispozitive mobile

9.3. Documentarea modificărilor

9.3.1. Toate revizuirile și actualizările trebuie documentate, inclusiv data revizuirii, modificările efectuate și aprobarea GM

9.3.2. Un istoric al versiunilor trebuie păstrat în scop de audit

9.4. Comunicare și acces

9.4.1. GM trebuie să se asigure că toți utilizatorii (angajați, contractori, terți) sunt informați cu privire la modificări

9.4.2. Versiunile actualizate trebuie puse la dispoziție într-un mod ușor accesibil, cum ar fi în foldere partajate sau pe platforme interne

10. Politici conexe și interdependențe

10.1. Această politică face parte din ansamblul politicilor IMM privind securitatea informației și trebuie implementată împreună cu următoarele:

10.1.1. P4S – Politica de control al accesului: Definește cerințele pentru gestionarea accesului securizat la sisteme, inclusiv la cele accesate prin dispozitive mobile. Impune igiena parolelor și controale privind sesiunea.

10.1.2. P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: Asigură instruirea utilizatorilor cu privire la utilizarea sigură a dispozitivelor mobile, raportarea incidentelor și condițiile BYOD.

10.1.3. P17S – Politica de protecție a datelor și confidențialitate: Stabilește gestionarea conformă cu GDPR a datelor personale și a datelor companiei pe platforme mobile, în special atunci când dispozitivele personale sunt utilizate în scop de serviciu.

10.1.4. P9S – Politica de telemuncă: Aliniază așteptările privind utilizarea mobilă atunci când se lucrează în afara sediului sau de la domiciliu, inclusiv cerințele privind gestionarea dispozitivelor și măsurile de protecție pentru accesul la rețea.

10.1.5. P30S – Politica de răspuns la incidente: Oferă cadrul de răspuns pentru incidentele legate de dispozitive mobile, inclusiv dispozitive compromise sau pierdute.

10.2. Aceste politici conexe funcționează împreună pentru a forma un set complet de controale pentru securitatea dispozitivelor mobile în IMM-uri fără personal IT dedicat, asigurând aplicabilitate, transparență și pregătire pentru certificare.

11. Standarde și cadre de referință

11.1. Această politică sprijină alinierea deplină cu următoarele standarde de securitate și conformitate:

11.2. ISO/IEC 27001:

11.2.1. Clauza 5.1 – Leadership și angajament: Asigură supravegherea de către management și responsabilitatea pentru accesul mobil și BYOD

11.2.2. Clauza 6.1 – Acțiuni pentru tratarea riscurilor: Impune evaluarea și tratarea riscurilor de securitate mobilă

11.2.3. Clauza 8.1 – Planificare și control operațional: Impune proceduri consecvente privind accesul mobil pentru protejarea datelor organizației

11.3. ISO/IEC 27002:

11.3.1. Controalele 5.10 (Utilizarea dispozitivelor mobile), 5.11 (Telemuncă), 5.12 (Acces la distanță) și 5.13 (BYOD): Oferă îndrumări de implementare pentru gestionarea riscurilor legate de dispozitive în contextul unei întreprinderi mici

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Controlul accesului pentru dispozitive mobile: Impune setări de securitate pentru utilizarea mobilă autorizată

11.4.2. AC-20 – Utilizarea sistemelor externe: Reglementează riscurile BYOD și de acces la distanță

11.4.3. CM-6 – Setări de configurare: Impune setări securizate implicite și particularizate pe platformele mobile

11.4.4. MP-7 – Utilizarea mediilor de stocare: Abordează utilizarea corectă și restricțiile privind stocarea mobilă și accesul la date

11.5. GDPR al UE (2016/679):

11.5.1. Articolul 5(1)(f) – Integritate și confidențialitate: Impune protecția datelor printr-un nivel adecvat de securitate a datelor cu caracter personal, în special pe platformele mobile

11.5.2. Articolul 32 – Securitatea prelucrării: Obligă utilizarea unor măsuri tehnice și organizatorice adecvate pentru securizarea datelor accesate sau stocate pe dispozitive mobile

11.6. Directiva NIS2 a UE (2022/2555):

11.6.1. Articolul 21(2)(d) – Măsuri de securitate pentru dispozitive: Impune controale de securitate pentru hardware-ul și software-ul utilizat pentru accesarea sistemelor critice ale organizației, inclusiv dispozitivele personale

11.7. DORA a UE (2022/2554):

11.7.1. Articolul 9 – Cadrul de management al riscurilor TIC: Impune protejarea terminalelor mobile utilizate pentru comunicații critice ale organizației și servicii cloud

11.7.2. Articolul 10 – Continuitatea activității TIC: Impune menținerea accesului securizat la sistemele organizației chiar și în timpul perturbărilor sau al lucrului la distanță

11.8. COBIT 2019:

11.8.1. APO13 – Gestionarea securității: Impune organizației să aplice politici privind dispozitivele mobile și BYOD aliniate la riscul corporativ

11.8.2. DSS01 – Gestionarea operațiunilor: Asigură implementarea tehnică a mecanismelor de acces securizat

11.8.3. DSS05 – Gestionarea serviciilor de securitate: Reglementează implicarea terților în menținerea unor medii mobile securizate și coordonarea răspunsului la incidente