					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P34					Titlul documentului: **Politica privind dispozitivele mobile și utilizarea dispozitivelor personale (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	5.2, 6.1, 7.5, 8	Se aplică controale de securitate și cerințe de conformitate
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Oferă controale detaliate pentru managementul dispozitivelor mobile
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Cerințe privind controlul accesului, accesul la distanță, configurarea și securitatea dispozitivelor mobile
GDPR al UE	5(1)(f), 25, 32	Cerințe obligatorii privind confidențialitatea, criptarea datelor și securitatea prelucrării
Directiva NIS2 a UE	21(2)(d)	Măsuri tehnice și organizatorice de protecție pentru accesul mobil
Regulamentul DORA al UE	9, 10	Managementul riscurilor TIC și cerințe de securitate pentru dispozitive mobile
COBIT 2019	APO13.02, DSS01.04, BAI09	Planuri de securitate a informațiilor, configurarea activelor și controale pentru medii mobile

1. Scop

1.1 Această politică stabilește cerințele de securitate, conformitate și operaționale pentru utilizarea dispozitivelor mobile și a tehnologiilor personale [utilizarea dispozitivelor personale (BYOD)] la accesarea sistemelor, aplicațiilor sau datelor organizației.

1.2 Scopul acesteia este de a asigura confidențialitatea, integritatea și disponibilitatea (CIA) informațiilor companiei accesate sau prelucrate prin terminale mobile, inclusiv smartphone-uri, tablete, laptopuri și dispozitive hibride.

1.3 De asemenea, această politică impune controalele tehnice și procedurale necesare pentru atenuarea riscurilor, precum scurgerile de date, accesul neautorizat, pierderea sau furtul dispozitivelor și compromiterea aplicațiilor mobile.

1.4 Această politică sprijină conformitatea cu cerințele de reglementare și contractuale, permițând totodată utilizarea în condiții de securitate a dispozitivelor mobile de către angajați, contractori și terți autorizați.

2. Domeniu de aplicare

2.1 Această politică se aplică întregului personal, inclusiv angajaților, contractorilor, stagiarilor și furnizorilor terți de servicii, care utilizează dispozitive mobile pentru a accesa datele, sistemele, aplicațiile sau platformele de comunicare ale companiei.

2.2 Politica acoperă toate dispozitivele mobile de calcul, inclusiv, fără a se limita la:

2.2.1 smartphone-uri și tablete (iOS, Android etc.)

2.2.2 laptopuri și ultrabook-uri (Windows, macOS, Linux)

2.2.3 dispozitive purtabile și dispozitive inteligente hibride capabile să sincronizeze date

2.3 Aceasta se aplică indiferent dacă dispozitivul este deținut de companie sau este deținut personal în baza unui acord BYOD.

2.4 Politica include toți vectorii de acces, inclusiv VPN, infrastructură de desktop virtual (VDI), aplicații cloud, poștă electronică, platforme de colaborare (de ex., SharePoint, Teams) și instrumente de sincronizare a fișierelor (de ex., OneDrive, Dropbox, dacă sunt autorizate).

2.5 Aceasta include utilizarea în regim de lucru la distanță, la sediu, în deplasare sau în aranjamente de lucru hibride.

3. Obiective

3.1 Reducerea riscului de compromitere, scurgere sau pierdere a datelor ca urmare a utilizării nesigure a dispozitivelor mobile.

3.2 Impunerea unor controale de securitate consecvente și aplicabile pentru toate terminalele mobile, indiferent de modelul de proprietate (corporativ sau BYOD).

3.3 Asigurarea faptului că utilizarea dispozitivelor mobile respectă ISO/IEC 27001 și alte cadre de reglementare aplicabile în materie de confidențialitate, protecția datelor și securitate cibernetică.

3.4 Facilitarea integrării securizate a dispozitivelor mobile în fluxurile operaționale, de comunicare și de colaborare ale organizației.

3.5 Asigurarea unor responsabilități și procese clar definite pentru managementul dispozitivelor mobile (MDM), inclusiv înrolarea, ștergerea la distanță, criptarea, autentificarea și monitorizarea.

3.6 Protejarea drepturilor la confidențialitate ale persoanelor care utilizează propriile dispozitive, menținând în același timp protecția informațiilor sensibile ale organizației.

4. Roluri și responsabilități

4.1 Directorul pentru securitatea informațiilor (CISO) / responsabilul cu securitatea IT

4.1.1 Definește politica și standardele tehnice pentru utilizarea dispozitivelor mobile și pentru utilizarea dispozitivelor personale (BYOD).

4.1.2 Asigură supravegherea conformității, a răspunsului la incidente și a gestionării excepțiilor pentru controalele aferente dispozitivelor mobile.

4.1.3 Coordonează activitățile cu departamentele juridic și de resurse umane pentru a se asigura că aplicarea este solidă din punct de vedere juridic și aliniată organizațional.

4.2 Administratorul IT / administratorul MDM

4.2.1 Gestionează alocarea accesului pentru dispozitive mobile, înrolarea și configurarea acestora prin soluții MDM.

4.2.2 Aplică controale la nivel de dispozitiv (de ex., criptare, coduri PIN, controale asupra aplicațiilor).

4.2.3 Efectuează ștergerea la distanță, blocarea și revocarea accesului atunci când este necesar.

[... 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 Această politică trebuie revizuită cel puțin anual de CISO sau de managerul securității informațiilor desemnat, pentru a asigura alinierea cu:

9.1.1 schimbările privind platformele de sisteme de operare mobile, tehnologiile MDM sau standardele de autentificare

9.1.2 modificările de reglementare sau contractuale care afectează protecția datelor mobile (de ex., GDPR, DORA, NIS2)

9.1.3 revizuirile seturilor de controale din ISO/IEC 27001:2022, ISO/IEC 27002:2022 sau NIST SP 800-53 Rev.5

9.1.4 feedbackul provenit din audituri, analize post-incident sau raportările angajaților

9.2 Revizuirile intermediare pot fi declanșate de:

9.2.1 incidente de securitate care implică dispozitive mobile sau platforme BYOD

9.2.2 notificarea de către furnizor a unor vulnerabilități cu risc ridicat în platformele suportate

9.2.3 introducerea unor noi aplicații mobile sau platforme de colaborare utilizate pentru activitățile operaționale ale organizației

9.3 Actualizările politicii trebuie să fie:

9.3.1 documentate în istoricul versiunilor politicii

9.3.2 comunicate întregului personal și contractorilor afectați

9.3.3 reconfirmate printr-o confirmare actualizată de luare la cunoștință pentru toți utilizatorii BYOD

9.4 Toate revizuirile și modificările trebuie aprobate formal de managementul executiv și înregistrate în registrul modificărilor de politică.

10. Politici conexe și interdependențe

10.1 Această politică este interdependentă cu mai multe politici-cheie din cadrul Sistemului de management al securității informațiilor (SMSI) al organizației. Interdependențele notabile includ:

10.1.1 P1 – Politica de securitate a informațiilor: stabilește principiile generale de guvernanță pentru toate controalele de securitate a informațiilor, inclusiv cele care reglementează utilizarea dispozitivelor mobile.

10.1.2 P3 – Politica de utilizare acceptabilă: definește comportamentele permise și restricțiile privind utilizarea tehnologiei, care se aplică direct accesului mobil și BYOD.

10.1.3 P9 – Politica de telemuncă: stabilește obligații suplimentare de securitate pentru mediile de lucru mobile, completând controalele specifice dispozitivelor mobile definite în această politică.

10.1.4 P13 – Politica de clasificare și etichetare a datelor: reglementează modul în care datele de pe dispozitivele mobile trebuie gestionate în funcție de nivelul de clasificare, influențând stocarea, transferul și aplicarea criptării.

10.1.5 P22 – Politica de jurnalizare și monitorizare: sprijină colectarea și revizuirea jurnalelor de acces mobil pentru detectarea anomaliilor sau a încălcărilor.

10.1.6 P30 – Politica de răspuns la incidente: reglementează modul în care incidentele legate de dispozitive mobile (de ex., pierderea dispozitivelor, acces neautorizat) sunt gestionate și escaladate.

10.1.7 P33 – Politica de audit și monitorizare a conformității: oferă baza pentru verificările periodice privind conformitatea securității mobile, inclusiv respectarea politicii BYOD.

11. Standarde și cadre de referință

11.1 Această politică este aliniată la cadre de securitate cibernetică recunoscute la nivel internațional și la obligații legale, pentru a asigura utilizarea securizată a dispozitivelor mobile și a tehnologiilor personale [utilizarea dispozitivelor personale (BYOD)] în mediile organizaționale.

11.2 ISO/IEC 27001:

11.2.1 Clauza 5.10 – utilizarea acceptabilă a activelor corporative: impune controale pentru utilizarea responsabilă a activelor corporative, inclusiv a dispozitivelor mobile.

11.2.2 Clauza 5.11 – lucrul la distanță: reglementează practicile sigure pentru accesarea sistemelor din afara spațiilor companiei.

11.2.3 Clauza 5.12 – utilizarea dispozitivelor mobile: impune controale bazate pe risc pentru terminalele mobile și configurațiile BYOD.

11.2.4 Clauza 5.13 – transferul informațiilor: impune protecția informațiilor transferate prin canale mobile.

11.3 ISO/IEC 27002:2022 – controalele 5.10–5.13:

11.3.1 Controalele din Anexa A 5.10–5.13 specifică modul în care accesul mobil, criptarea, monitorizarea și atenuarea pierderilor trebuie aplicate în cadrul unui Sistem de management al securității informațiilor (SMSI). Aceste controale oferă îndrumări detaliate de implementare pentru securizarea terminalelor mobile, aplicarea containerizării, monitorizarea integrității dispozitivelor și asigurarea unor configurații BYOD conforme cu cerințele de confidențialitate.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – controlul accesului pentru dispozitive mobile: definește protecțiile de bază, inclusiv criptarea, autentificarea și aplicarea MDM.

11.4.2 AC-17 – acces la distanță: impune autentificare securizată și protecția sesiunilor pentru utilizatorii mobili la distanță.

11.4.3 CM-7 – funcționalitate minimă: sprijină eliminarea aplicațiilor și funcțiilor nenecesare de pe terminalele mobile pentru reducerea riscului.

11.4.4 MP-5 – protecția transportului mediilor: reglementează transmiterea securizată a datelor de la sistemele mobile către destinații externe sau din cloud.

11.4.5 SC-12 – stabilirea cheilor criptografice: impune utilizarea protocoalelor criptografice securizate pentru comunicațiile și stocarea pe dispozitive mobile.

11.5 GDPR al UE (2016/679):

11.5.1 Articolul 5(1)(f) – integritate și confidențialitate: impune organizațiilor să protejeze datele cu caracter personal de pe dispozitivele mobile împotriva accesului neautorizat sau ilegal.

11.5.2 Articolul 25 – protecția datelor încă din faza de proiectare și în mod implicit: impune integrarea confidențialității în procesele BYOD și MDM.

11.5.3 Articolul 32 – securitatea prelucrării: impune controale bazate pe risc (de ex., criptare, autentificare, controlul accesului) pentru datele cu caracter personal pe platforme mobile.

11.6 Directiva NIS2 a UE (2022/2555):

11.6.1 Articolul 21(2)(d): impune ca accesul mobil la sisteme și informații critice să fie protejat prin măsuri tehnice și organizatorice adecvate, cum ar fi controlul terminalelor, criptarea și monitorizarea.

11.7 Regulamentul DORA al UE (2022/2554):

11.7.1 Articolul 9 – cadrul de management al riscurilor TIC: impune entităților din sectorul financiar să atenueze riscurile asociate accesului mobil și accesului la distanță ca parte a rezilienței operaționale.

11.7.2 Articolul 10 – cerințe de securitate pentru sistemele TIC: impune o arhitectură mobilă securizată, mecanisme de monitorizare și mecanisme de răspuns pentru amenințările cibernetice inițiate de pe dispozitive mobile.

11.8 COBIT 2019:

11.8.1 APO13.02 – stabilirea și menținerea unui plan de securitate a informațiilor: impune integrarea utilizării dispozitivelor mobile, inclusiv BYOD, în strategiile de securitate ale organizației.

11.8.2 DSS01.04 – gestionarea configurației și integrității activelor: se aplică controlului configurației și implementării securizate a dispozitivelor mobile.

11.8.3 BAI09.01 – stabilirea și menținerea controalelor: sprijină implementarea măsurilor tehnice și procedurale de protecție pentru operațiuni mobile și la distanță în condiții de securitate.