

Politica privind utilizarea dispozitivelor mobile

Pentru Societatea CLEAN RECYCLE S.A.

1. Introducere

Dispozitivele mobile reprezintă o componentă tot mai mare a vieții de zi cu zi, deoarece dispozitivele devin mai mici și mai puternice, iar numărul de sarcini care pot fi îndeplinite cu ajutorul lor și departe de birou crește. Cu toate acestea, pe măsură ce capacitățile cresc, în mod evident, cresc și riscurile. Comenzile de securitate care protejează mediul desktop static nu sunt la fel de sigure atunci când se utilizează un dispozitiv mobil în afara limitelor unei clădiri de birouri.

Ca exemple de dispozitive mobile, putem enumera:

- Laptopuri.
- Notebookuri.
- Tablete.
- Smartphone-uri.
- Ceasuri inteligente.

Scopul acestei politici este de a stabili măsurile care trebuie să fie utilizate atunci când se utilizează dispozitive mobile. Se intenționează să se reducă următoarele riscuri:

- Pierderea sau furtul de dispozitive mobile, inclusiv datele pe care acestea le conțin.
- Compromiterea informațiilor clasificate prin acces neautorizat.
- Introducerea în rețea a virușilor sau a programelor malware.
- Pierderea reputației.

Este important ca măsurile stabilite în această politică să fie respectate în orice moment în utilizarea și transportul dispozitivelor mobile.

Această politică se aplică tuturor sistemelor, persoanelor și proceselor care constituie sistemele informatice ale organizației, inclusiv membrii consiliului, directorii, angajații, furnizorii și alte părți terțe care au acces la sistemele Societății.

2. Politica privind dispozitivele mobile

2.1. Dispozitive furnizate de Societate

În lipsa unei aprobări prealabile a conducerii, numai dispozitivele mobile furnizate de Societate trebuie folosite pentru a ține sau a procesa informații clasificate în numele societății.

Dacă se solicită utilizarea echipamentele mobile se va oferi un dispozitiv corespunzător care va fi configurat să respecte politicile organizației. Sprijinul va fi oferit de către [Biroul de suport tehnic](#), care poate avea uneori nevoie de acces la dispozitiv pentru rezolvarea problemelor și pentru mentenanță.

Trebuie să se asigure că dispozitivul este transportat și depozitat în medii sigure și nu este expus unor situații în care acesta se poate deteriora. Nu se va lăsa aparatul nesupravegheat la vederea publicului, cum ar fi în spatele unei mașini, într-o sală de ședințe sau în hol.

Nu se va elimina niciun semn de identificare de pe dispozitiv, cum ar fi o etichetă a companiei sau o serie. Se vor lua măsuri ca dispozitivul să fie blocat și protejat de o parolă puternică.

Nu se va adăuga echipament hardware periferic fără aprobarea [sefului biroului suport tehnic](#). [Seful biroului suport tehnic](#) trebuie să fie consultat înainte ca aparatul să fie scos din țară.

Nu se vor stoca informații confidențiale pe dispozitiv (cum ar fi date cu caracter personal) decât dacă acest lucru a fost autorizat și dacă măsurile adecvate (de exemplu criptarea) au fost introduse. Nu se va păstra dispozitivul parolele de acces, numerele de identificare personale sau alte elemente de securitate la vedere sau ușor accesibile.

Asigurați-vă că ecranul dispozitivului se blochează după o scurtă perioadă de neutilizare și necesită un cod de acces sau o parolă pentru a-l debloca. Parolele utilizate trebuie să fie puternice și greu de ghicit. Nu se pot seta pe dispozitiv niciun fel de conectări neasigurate (adică cele care nu necesită o parolă).

Dispozitivul furnizat de societate este destinat exclusiv destinației indicate: nu trebuie să fie împărtășită cu familia sau prietenii sau folosit pentru activități personale. Este posibil să vi se solicite să returnați dispozitivul la [Biroul de suport tehnic](#) în orice moment pentru inspecție și audit. Nu trebuie să instalați niciun software neautorizat sau să schimbați configurația sau setarea dispozitivului fără a consulta mai întâi [Biroul de suport tehnic](#).

Acolo unde este posibil, dispozitivul va fi securizat astfel încât toate datele de pe acesta să fie criptate și să fie accesibil doar dacă parola este cunoscută. Dacă dispozitivul este livrat cu criptare, nu dezactivați criptarea.

Este posibil ca modificările aduse fișierelor deținute pe dispozitiv să nu fie însoțite în mod regulat dacă nu sunt conectate la rețeaua corporativă pentru o perioadă de timp. Încercați să programați ceva timp pentru a realiza acest lucru în mod regulat. Nu țineți propriile backup-uri necriptate de informații clasificate.

Dacă este cazul, protecția împotriva virusurilor va fi instalată pe dispozitiv de către organizație. Asigurați-vă că dispozitivul este conectat periodic la rețeaua companiei pentru a permite actualizarea anti-virusului. Nu dezactivați protecția antivirus.

Dispozitivul nu trebuie să fie conectat la rețele non-corporative, cum ar fi wireless sau Internet, cu excepția cazului în care este utilizată o rețea VPN (Virtual Private Network/Rețea Virtuală Privată). Când vă aflați în locuri publice, asigurați-vă că ați amplasat dispozitivul astfel încât utilizatorii neautorizați să nu poată vizualiza ecranul sau să facă fotografii sau videoclipuri ecranului.

2.2. Utilizarea dispozitivelor mobile personale

Costul redus și disponibilitatea generală a unor astfel de dispozitive au alimentat dorința angajaților și a altor părți interesate de a-și folosi propriile dispozitive pentru a le folosi în scopuri comerciale. Aceasta este denumită în mod obișnuit „*Îți aduci propriul dispozitiv*” (BYOD). În unele cazuri, acest lucru poate oferi o flexibilitate sporită și poate elimina necesitatea ca angajatul să transporte mai multe dispozitive în mod regulat.

Cu toate acestea, conceptul de a permite unui angajat să utilizeze propriul dispozitiv (dispozitive) în scopuri de afaceri poate avea ca rezultat necesitatea ca astfel de dispozitive să fie supuse unor controale suplimentare în plus față de cele care există în mod obișnuit pentru un dispozitiv de consum.

Problemele comune și problemele de securitate cu BYOD pot include:

- utilizarea aparatului de către alți membri ai familiei
- stocarea implicită a datelor în facilitățile copiilor de rezervă în cloud
- expunerea crescută la pierderi potențiale în situații sociale, de ex. pe plajă, într-un bar
- acces potențial la site-uri care nu respectă politica de utilizare acceptabilă a organizațiilor
- conectarea la rețele nesigure, de exemplu rețele wireless nesecurizate
- inexistența unui anti-virus
- instalarea de aplicații potențial dăunătoare pe dispozitiv (de multe ori fără ca utilizatorul să fie conștient de faptul că este malware)

Aceste aspecte trebuie luate în considerare atunci când se evaluează caracterul adecvat al oricărui dispozitiv de a stoca datele confidențialele societății.

Proprietarul dispozitivului și organizația vor decide dacă un anumit dispozitiv va fi utilizat în activitatea desfășurată de angajat. Această utilizare nu este obligatorie, iar angajatul are dreptul de a decide dacă controalele suplimentare introduse pe dispozitiv de către organizație sunt acceptabile și, prin urmare, dacă aceștia aleg să utilizeze dispozitivul în scopul propus.

Este important ca măsurile stabilite în această politică să fie respectate în orice moment în utilizarea și transportul dispozitivelor mobile BYOD. Persoanele fizice nu trebuie să utilizeze propriile dispozitive pentru a ține și prelucra informații despre companie decât dacă au depus o cerere în acest sens și această solicitare a fost aprobată oficial. Este politica Institutiei să evalueze fiecare cerere BYOD în mod individual, pentru a stabili:

- identitatea persoanei care face cererea;
- motivul cererii;
- datele care vor fi păstrate sau procesate pe dispozitiv;
- dispozitivul specific care va fi utilizat;

Solicitările trebuie trimise la **Biroul de suport tehnic**.

Principiul general al acestei politici este că gradul de control exercitat de organizație asupra dispozitivului BYOD va fi proporțional cu gradul sensibilității datelor deținute de acesta.

Pentru a asigura că datele sale sunt protejate în mod adecvat, este important ca Societatea să poată monitoriza și să verifice nivelul de conformitate cu această politică. Nivelul de monitorizare și de audit va fi adecvat clasificării informațiilor deținute pe dispozitiv.

Metodele și calendarul monitorizării și auditului vor fi astfel încât intimitatea proprietarului dispozitivului să nu fie afectată și, în toate cazurile, cu respectarea legislației în materia protecției datelor cu caracter personal. În general, monitorizarea utilizării în afara programului de lucru va fi evitată.

În cazul în care dispozitivul este pierdut sau furat, proprietarul trebuie să informeze **Biroul de suport tehnic** cât mai curând posibil, oferind detalii despre circumstanțele pierderii și sensibilitatea informațiilor de afaceri stocate pe acesta. Societatea își rezervă dreptul de a șterge de la distanță dispozitivul, dacă este posibil, ca măsură de precauție. Aceasta poate implica ștergerea datelor personale ale proprietarului dispozitivului.

La părăsirea societății, proprietarul dispozitivului trebuie să permită ca dispozitivul să fie auditat și să fie eliminate toate datele și aplicațiile companiei.

| Nivel de Protecție | Categoriile de informații | Cine poate avea acces prin BYOD | Tipuri dispozitive BYOD | Controale necesare | Comentarii |
|----------------------------------|--|---|--|--|--|
| Nivelul 0 - Public | Cataloage de produse, informații despre prețuri, adrese de locație ale Instituției și numere de contact | Oricine | Oricare | Nici unul | Aceste informații sunt în general accesibile publicului și accesate prin mijloace accesibile publicului, de exemplu un site web. |
| Nivelul 1 - Protejat | Proceduri interne, detalii despre produs, comunicații interne ale societății, e-mail necondiționat sau confidențial. | Angajați și alte părți interesate autorizate. | Laptopuri Tablete Dispozitive smartphone | Protecție prin parolă pentru dispozitiv Blocare inactivă Ștergere de la distanță Protecția prin parolă pentru aplicație Audituri periodice | Această zonă este cea mai folosită utilizare a BYOD din cadrul societății. |
| Nivelul 2 - Restricționat | Resurse umane, informații bancare, date cu caracter personal protejate de | Grupuri restrânse de angajați | Doar laptopuri | Criptare completă pe disc Rețea VPN | Aceste informații trebuie accesate numai prin dispozitive cu controale stricte de securitate. Acest lucru poate împiedica practic utilizarea |

| | | | | | | |
|---------------------------------|--|--------|-----------|--|---|--|
| | legislația privind protecția datelor | | | | Colare automatizată Antivirus Sistem Firewall Audituri periodice | unui dispozitiv BYOD în funcție de circumstanțe. |
| Nivelul 3 - Confidențial | Planuri de resurse ale companiei, propuneri comerciale, informații financiare nepublicate, alte secrete comerciale | Nimeni | Nici unul | | Nu se aplică | Aceste informații trebuie accesate numai prin intermediul unor dispozitive furnizate de organizație, cu controale stricte de securitate. |

Tabloul 1 - Ghidul BYOD

3. Consecințe

Nerespectarea prezentei Politici de către angajații societății sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse Societății ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), Societatea va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

Prezenta Politică va fi adusă de către conducerea Societății la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

| | |
|---|-----------|
| Politică aprobată în data de: |2021 |
| Politică devine operațională din data de: |2021 |
| Următoarea revizuire va avea loc în data de: |2022 |

Firma: CLEAN RECYCLE S.A.

Administrator: Monda Radu Cosmin

