



# GHID PRACTIC

**pentru angajatorii și  
angajații care implementează  
sisteme de lucru la distanță**

*Acest ghid prezintă un conținut informațional și recomandări de natură consultativă, fiind destinat să asiste angajatorii și angajații în organizarea și securizarea lucrului de la distanță.*



# Introducere

În contextul situației epidemiologice declanșată la nivel național și operarea mai multor modificări în organizarea procesului de lucru, Serviciul Tehnologia Informației și Securitate Cibernetică a elaborat un GHID practic și consultativ pentru angajatorii și angajații care implementează sisteme de lucru la distanță.

Dat fiind faptul că în această perioadă critică tot mai mulți angajați din sectorul public și privat operează de la distanță cu datele confidențiale ale instituției/organizației în vederea realizării sarcinilor de serviciu și utilizează în activitatea curentă diverse soluții pentru video conferințe (ex. Zoom, Cisco Webex și Google Met) sau aplicații de mesagerie (ex. Snapchat, WhatsApp, Telegram și Semnal), este foarte important să fie evaluate corect riscurile de securitate și respectiv organizată asistența tehnică și informațională a angajaților, respectând nemijlocit cerințele minime de securitate cibernetică în procesul de lucru.







# ORGANIZAREA, ASISTAREA TEHNICĂ ȘI INFORMAȚIONALĂ A ANGAJAȚILOR

- **INSTRUIȚI** și acordați asistență angajaților în cazul în care aceștia întâmpină dificultăți, privind modul de utilizare a instrumentelor de lucru la distanță (ex. acces la proceduri operaționale în caz de urgență, persoana desemnată responsabilă și orele de lucru când poate fi apelată).
- **RESTRICȚIONAȚI** accesului la sisteme cu nivel de protecție scăzut.
- **IMPLEMENTAȚI** proceduri de autorizare ce ar permite utilizarea dispozitivelor personale ale angajatului (BYOD).
- **ORGANIZAȚI** accesul de la distanță doar prin intermediul rețelei virtuale private (VPN) sau alte soluții similare.
- **MONITORIZAȚI** regulat realizarea copiilor de rezervă pentru toate fișierele importante ale companiei/instituției.
- **VERIFICAȚI** și testați capacitatea infrastructurii IT în raport cu numărul de utilizatori care necesită acces simultan.
- **ADOPTAȚI** măsuri de securitate privind contracararea acțiunilor frauduloase ale atacatorilor cibernetici care ar încerca să exploateze situația generată de lucrul la distanță, inclusiv prin propagarea ransomware și utilizarea unor tehnici de phishing având ca pretext informații despre pandemie.
- **UTILIZAȚI** soluții sigure de certificare, precum semnătura electronică avansat calificată pentru a putea semna electronic diverse documente prin intermediul Serviciului MSign ([msign.gov.md](https://msign.gov.md)) și respectiv organiza circuitul electronic al acestor documente la nivel instituțional sau interinstituțional.

**!! Actualizarea automată a stațiilor de lucru ale angajaților se cere a fi realizată și atunci când angajații lucrează de la distanță.**



# SECURIZAREA MEDIULUI DE LUCRU

Lucrul de la distanță, prin utilizarea dispozitivelor personale, presupune riscuri suplimentare, deoarece întotdeauna va exista posibilitatea ca un atacator cibernetic să obțină acces fizic la unul din aceste dispozitive și respectiv acces la date confidențiale de caracter personal sau ale companiei



- **Deconectați aplicațiile folosite**, atunci când nu folosiți dispozitivul, atât acasă, cât și în locurile publice. Situația nedorită în care un copil curios poate trimite accidental un e-mail poate fi evitată cu ușurință, de asemenea, accesul unei persoane străine la informațiile afișate pe ecran este blocat, eliminând orice risc într-un spațiu public.
- **Blocați dispozitivul**, pentru a evita situații neplăcute și a păstra în siguranță dispozitivul, accesul fiind posibil doar prin parolă. În caz de părăsire a mesei de lucru, utilizați pentru blocarea ecranului dispozitivului combinația de taste **Windows+L** din Windows și combinația **Ctrl + Cmd + Q** pentru Mac.
- **Implementați o politică puternică de parole**, folosind parole puternice și utilizând Generatorul de parole pentru a crea parole securizate, ce sunt dificil de spart sau de ghicit. În cazul în care folosiți aceeași parolă pentru mai multe conturi, este suficient să fie compromisă doar una din ele, pentru ca un infractor să preia acces la toate conturile. Parolele trebuie să fie unice pentru fiecare cont și să cuprindă un șir lung (minim 8 caractere) de litere mari și minuscule, numere și caractere speciale. Puteți folosi și autentificarea în doi pași (2FA), în special în cazul conturilor de e-mail și social media.







- **Efectuați regulat copii de rezervă a datelor.** Datele pot fi pierdute în mai multe moduri, inclusiv erori umane, daune fizice a hardware-ului sau un atac cibernetic. Ransomware-ul și alte tipuri de malware pot șterge sisteme întregi fără a putea fi detectate. Copia de rezervă hardware este prima opțiune, iar opțiunea alternativă și printre cele mai convenabile și mai eficiente metode de stocare a datelor este în Cloud. Serviciile de backup Cloud oferă o multitudine de opțiuni care vă permit să vă personalizați programul de backup și opțiunile de stocare.
- **Securizați router-ul de acasă.** După cum arată experiența, foarte multe persoane nu schimbă parola router-ului atunci când este instalat/configurat pentru prima dată (folosind parola implicită de la producător), lăsând astfel rețeaua de la domiciliu vulnerabilă. Pentru a evita acest lucru, este necesar de schimbat parola router-ului și de configurat criptările WPA2 sau WPA3 pentru Wi-Fi. Limitați traficul de intrare și de ieșire, utilizați cel mai înalt nivel de criptare disponibil și opriți WPS.
- **Atenție la e-mail-uri și site-uri phishing.** Din cauza focarului de COVID-19, este foarte probabil ca e-mail-urile de tip phishing să vizeze lucrătorii care muncesc la distanță în scopul de a le fura informațiile personale sau de a avea acces la conturile companiei. Semnele obișnuite ale unui email sau site de phishing sunt erori gramaticale în subiect, lipsa unui simbol al lacătului HTTPS, nume de domeniu scris greșit, lipsa unei pagini „despre” și lipsă de informații de contact.

#### ATENȚIE!


Criptarea full-disk este o soluție simplă, dar puternică, asigurându-vă că în situația în care laptopurile sunt pierdute sau furate, datele companiei nu sunt compromise.




# SECURIZAREA ACCESULUI DE LA DISTANȚĂ LA REȚEA



- Utilizarea rețelei de VPN pentru a conecta angajații de la distanță la rețeaua internă a organizației. Acest lucru împiedică atacurile, care se interpun fluxului de date transmise din locații îndepărtate.
- Obținerea accesului numai cu un echipament deținut de companie, astfel încât controlul complet al dispozitivului de conectare să fie sub controlul și monitorizarea echipei IT.
- Verificarea utilizării dispozitivelor externe, cum ar fi stocarea datelor pe USB și alte dispozitive periferice.
- Limitarea capacității de a stoca, descărca sau copia date. O breșă de date poate avea loc de la nivelul oricărui dispozitiv care stochează date sensibile.

 **!! În cazul în care o parte (sau toți) angajații dvs. utilizează dispozitive BYOD (personale), dacă le permiteți accesul la servicii de e-mail și cloud, asigurați-vă că aplicați aceeași politică de securitate anti-malware, firewall etc., ca atunci când utilizează un echipament al organizației/instituției.**

 **!! Dacă este necesar, furnizați angajatului o licență similară cu cea utilizată pe dispozitivele deținute de companie. Dacă aveți nevoie de licențe suplimentare, contactați furnizorul. Este posibil să fie disponibile soluții care să vă protejeze în timpul acestui eveniment fără precedent.**







# STOCAREA DATELOR ÎN CLOUD

## Practici utile

Pentru multe organizații și instituții serviciile Cloud au înlocuit rețelele locale ale companiei pentru a stoca, gestiona și partaja informații. Deși tranziția lucrului de la birou la domiciliu este cu siguranță mai ușoară prin stocarea în Cloud, există totuși anumite probleme de securitate care trebuie abordate pentru a bloca informațiile Dvs. sensibile.

Majoritatea preocupărilor se concentrează în jurul riscurilor percepute de a permite altei entități terțe să vă găzduiască datele. Și, deoarece este stocat în Cloud („în nori”), există riscul că poate fi accesat de oricine de pe Internet cu datele de acreditare corecte. În cel mai rău caz, acesta ar putea fi un atacator care cuprinde un laptop de utilizator sau ghicește o parolă slabă.

### ATENȚIE!

Documentele trebuie structurate și blocate cu permisiuni de acces adecvate pentru a se asigura că numai utilizatorii autorizați să vizualizeze conținutul pot face acest lucru. De exemplu, puteți restricționa accesul și partajarea cu persoane din afara rețelei corporative, accesul fiind oferit numai angajaților din companie. Pentru un plus de securitate, se recomandă utilizarea autentificării cu 2 factori (2FA) pentru conturile online (ex. Google, Microsoft, Apple, Yahoo, LinkedIn, Facebook, etc.) Deși 2FA nu reprezintă un înlocuitor pentru o parolă sigură, este un alt nivel de securitate care vă ajută să păstrați siguranța conturilor importante.





I.P. Serviciul Tehnologia Informației și Securitate Cibernetică  
MD-2012, or. Chișinău, Republica Moldova  
Piața Marii Adunări Naționale 1



[www.stisc.gov.md](http://www.stisc.gov.md)



(022) 820 911



[stisc@stisc.gov.md](mailto:stisc@stisc.gov.md)  
[infor@cert.gov.md](mailto:infor@cert.gov.md)

