

# Politica privind securitatea informației

## 1. Scop

Prezentul document are scopul de a conștientiza și familiariza personalul Instituției cu privire la metodele de protecție și securitate pentru asigurarea confidențialității, integrității și disponibilității informației. De asemenea, documentul conturează metodele acceptabile de utilizare a resurselor informatice. Resursele informaționale vor fi utilizate într-o manieră aprobată, etică și în conformitate cu prevederile legale pentru a evita pierderea sau deteriorarea operațiunilor curente, a imaginii sau a activelor financiare. Angajații trebuie să se adreseze conducerii instituției înainte să se angajeze în orice activitate care nu este acoperită de prezenta politică.

## 2. Domeniul de aplicabilitate

Această Politică se aplică întregului personal, partenerilor și afaceri și colaboratorilor externi care au acces la sistemul informatic al Instituției.

## 3. Obiective

- a) Dezvoltarea unei strategii privind securitatea sistemelor informatice;
- b) Promovarea standardelor etice în domeniul securității sistemelor informatice;
- c) Asigurarea confidențialității, integrității și disponibilității resurselor informatice ale organizației;
- d) Educarea personalului pentru a face față eficient amenințărilor cibernetice;
- e) Cunoașterea riscurilor și amenințărilor venite din spațiul cibernetic;
- f) Oferirea soluțiilor pentru a preveni și contracara amenințările cibernetice;

## 4. Securitatea informației

- 1. Accesul la echipamentele IT ale organizației de către terți se va face sub supraveghere. În contractele cu terți se vor include clauze privind măsurile de protecție a datelor și, în special, a datelor cu caracter personal;
- 2. Informațiile vor avea diferite grade de sensibilitate și importanță, informațiile personale (datele cu caracter personal) necesitând un nivel suplimentar de protecție;
- 3. Responsabilitatea angajaților privind securitatea va fi implementată încă din etapa recrutării și inclusă în contractele de muncă sau fișă postului și monitorizată permanent;
- 4. Parolele utilizate pentru autentificare sunt șiruri de caractere, adecvate din punct de vedere al securității ca lungime și compoziție, conținând majuscule și caractere speciale și sunt formate din cel puțin 8 caractere. Parolele nu sunt afișate pe monitor. Acestea sunt schimbate periodic, cel puțin o dată la două luni. Schimbarea periodică a parolilor se face numai de către utilizatori autorizați.

5. Angajații instituției sau alte terțe părți care au acces la sistemele informatice ale organizației ar trebui să semneze un contract de confidențialitate;
6. Angajații ar trebui să fie instruiți cu privire la Securitatea Informațiilor;
7. Toate incidentele de Securitate vor fi raportate conducerii, pentru a decide dacă este cazul ca acestea să fie raportate Autorității de Supraveghere și/sau persoanelor vizate. Se va implementa în acest sens o Politică privind managementul adecvat al incidentelor de Securitate;
8. Informațiile critice sau sensibile, precum și datele cu caracter personal trebuie să fie adăpostite în locuri sigure, protejate într-un perimetru de securitate adecvat, cu bariere de securitate corespunzătoare și controale de acces. Acestea ar trebui să fie protejate fizic împotriva accesului neautorizat, deteriorare și interferențe. Protecția oferită trebuie să fie proporțională cu riscurile identificate.
9. Sistemele IT vor fi protejate împotriva amenințărilor de Securitate și se vor implementa măsuri de securitate pentru a preveni și detecta accesul neautorizat în sistemele informatice și asupra datelor.
10. Trebuie să se introducă proceduri pentru efectuarea de back-up strategic, simularea periodică a restaurării de pe copiiile realizate, logarea evenimentelor și a defectelor, acolo unde este posibil și monitorizarea permanentă a echipamentelor critice.
11. Utilizarea oricărui sistem IT va fi conformă legislației în vigoare cât și a normelor interne.
12. Este strict interzisă distribuirea oricăror documente interne sau alte informații către persoane neautorizate;
13. Este strict interzisă orice modificare neautorizată a echipamentelor utilizate;
14. Este strict interzisă conectarea echipamentelor personale de orice fel (hard-diskuri interne sau externe, memory stick, laptop etc) la orice echipament al organizației (PC, server, rețea internă). Nerespectarea acestei reguli aduce după sine posibilitatea desfacerii contractului de muncă sau alte măsuri disciplinare.
15. Toate sursele externe (CD, atașamente la e-mail, stick-uri, hard-disk etc) vor fi verificate cu un program anti-virus.
16. Este strict interzisă utilizarea sistemelor IT în alte scopuri decât îndeplinirea atribuțiilor de serviciu.
17. Infrastructura IT (Servere, Echipamente rețea, website) vor fi scanate de vulnerabilități și raportul de risc va fi distribuit conducerii instituției și departamentului IT în vederea remedierii riscurilor în cel mai scurt timp. Scanările vor trebui efectuate periodic cu o recurență cel puțin semestrială.
18. Este interzisă orice intervenție asupra echipamentelor IT de către personal neautorizat de către instituție în mod scris.
19. Se interzice folosirea oricărui echipament IT de către orice persoană care nu face parte din personalul Instituției fără acordul prealabil și scris al conducerii Instituției.
20. Mijloacele de autentificare în sistem (username, parolă etc) sunt proprietatea fiecărui angajat și el este singurul responsabil de a nu divulga aceste informații. De asemenea se recomandă utilizarea de sisteme de autentificare cu dublu factor (SMS,Token,etc.)
21. Este strict interzisă utilizarea credențialelor altui angajat.

22. Fiecare angajat va fi responsabil să mențină securitatea oricărei informații, și în special informațiilor personale (datelor cu caracter personal) și să le protejeze de acces neautorizat (vizualizare, alterare, furt sau distrugere).
23. Pentru copierea fișierelor electronice, instituția își rezervă dreptul de a depune plângere penală împotriva angajatului și de a-l acționa pe acesta la instanțele civile pentru acoperirea oricărui prejudiciu adus instituției.
24. Este strict interzisă încălcarea drepturilor de autor.
25. Este interzisă navigarea prin fișierele personale sau conturile altor angajați, cu excepția cazului în care acest lucru a fost aprobat în prealabil.
26. Programatorii care vor dezvolta sisteme IT nu vor avea acces la date cu caracter personal, decât dacă acestea au fost anonimizate complet.
27. Personalul care asigură suportul tehnic nu va avea acces la date cu caracter personal, decât în situații excepționale și, în toate cazurile, cu respectarea tuturor obligațiilor impuse de Regulamentul (EU) 679/2016 persoanelor împuternicire și, în special, existența unor clauze contractuale exprese privind protecția datelor.
28. Notarea sau stocarea parolilor pe orice suport fizic este strict interzisă.
29. Sistemul trebuie blocat ori de câte ori angajatul părăsește biroul sau nu utilizează calculatorul.
30. După terminarea programului, calculatorul va fi închis.
31. Este strict interzisă utilizarea „Print screen-ului” (prin folosirea tastei print screen sau a altor procedee) sau prin fotografierea monitorului cu telefonul pentru a salva/imprima datele cu caracter personal existente pe monitor.
32. Listarea documentelor ce conțin date cu caracter personal se va realiza doar de către utilizatorii autorizați sau cu aprobarea scrisă și prealabilă a conducerii.
33. Se va realiza back-up periodic la toate informațiile stocate pe sistemele IT.
34. Angajații nu vor uita documente pe birou care conțin date cu caracter personal după terminarea programului sau în pauză.
35. Angajații vor lua din imprimantă documentele proprii imediat după tipărire.

## **5. Consecințe**

Nerespectarea prezentei Politici de către angajații instituției 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 Instituției ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

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