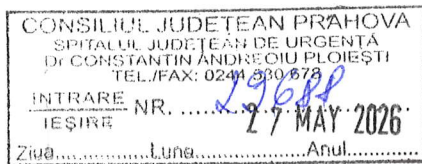




Spitalul Județean de Urgență
Dr. Constantin Andreoiu Ploiești
Str. Găgeni nr. 100
Tel: +40244537711, Fax: +40244530678
E-mail: secretariat@sjup.ro
Website: www.sjup.ro



Aprobat Manager,
Dr. Sebastian TOMA



POLITICA DE SECURITATE IT

Spitalul Județean de Urgență "Dr. Constantin Andreoiu" Ploiești

1. Scop, domeniu de aplicare și utilizatori

Scopul prezentului document este de a defini regulile și măsurile de securitate privind utilizarea sistemului informațional și protecția activelor informatice din cadrul Spitalului Județean de Urgență Dr. Constantin Andreoiu Ploiești, în conformitate cu legislația aplicabilă privind securitatea informației, protecția datelor cu caracter personal și securitatea cibernetică.

Prezenta politică se aplică tuturor angajaților, colaboratorilor, personalului contractual, rezidenților, studenților, furnizorilor și altor persoane care utilizează infrastructura IT sau au acces la informațiile și sistemele informatice ale spitalului.

2. Reguli generale de securitate

2.1. Definiții

Sistem informațional

Ansamblul serverelor, stațiilor de lucru, echipamentelor de rețea, aplicațiilor software, bazelor de date, sistemelor de comunicații și altor componente informatice utilizate de spital.

Active informatice

Totalitatea echipamentelor IT, documentelor electronice și fizice, suporturilor de stocare, conturilor de utilizator, dispozitivelor mobile și informațiilor aflate în administrarea spitalului.

2.2. Utilizare acceptabilă

Activele informatice ale spitalului vor fi utilizate exclusiv în scop profesional și pentru desfășurarea activităților specifice atribuțiilor de serviciu.

Este interzisă utilizarea resurselor IT în scop personal excesiv, ilegal sau care poate afecta securitatea, performanța sau imaginea spitalului.

2.3. Responsabilitatea pentru active

Fiecare activ informatic are un responsabil desemnat, conform inventarului IT al unității.

Responsabilul activului are obligația de a asigura:

- confidențialitatea;
- integritatea;
- disponibilitatea informațiilor gestionate.

2.4. Activități interzise

Sunt interzise:

- instalarea de software fără aprobarea Responsabilului IT;
- utilizarea de aplicații neautorizate;
- conectarea de dispozitive externe fără aprobare;
- utilizarea sistemelor informatice pentru activități ilegale;
- accesarea de site-uri nesigure sau necorespunzătoare activității profesionale;
- descărcarea neautorizată de materiale multimedia;
- parasirea unitatii sanitare cu echipamentul de serviciu (fara aprobarea prealabila a Conducerii);
- transmiterea de mesaje tip spam;
- dezactivarea soluțiilor antivirus sau a mecanismelor de securitate;



Spitalul Județean de Urgență
Dr. Constantin Andreoiu Ploiești
Str. Găgeni nr. 100
Tel: +40244537711, Fax: +40244530678
E-mail: secretariat@sjup.ro
Website: www.sjup.ro



- utilizarea neautorizată a dispozitivelor USB, hard diskurilor externe sau altor medii de stocare.

2.5. Utilizarea echipamentelor în afara spitalului

Echipamentele IT, documentele sau informațiile aparținând spitalului nu pot fi scoase din incinta unității fără aprobarea scrisă a conducerii sau a Responsabilului IT.

Persoana care utilizează echipamentele în exteriorul unității răspunde de securitatea și integritatea acestora, conform prevederilor legale.

2.6. Restituirea activelor

La încetarea raporturilor de muncă sau colaborare, utilizatorul are obligația de a restitui toate echipamentele, documentele, conturile și accesurile aferente activității desfășurate.

Responsabilul IT va dezactiva accesurile informatice imediat după încetarea raporturilor contractuale.

2.7. Copii de siguranță (Back-up)

Back-up-ul datelor critice se realizează periodic de către Compartimentul IT, conform procedurilor interne.

Utilizatorii au obligația de a salva datele importante în locațiile stabilite de spital și de a evita stocarea exclusivă pe stațiile locale de lucru.

2.8. Protecție antivirus și actualizări

Toate echipamentele conectate la rețeaua spitalului trebuie să utilizeze:

- soluții antivirus active și actualizate;
- actualizări automate de securitate;
- firewall activ.

Este interzisă dezactivarea mecanismelor de protecție fără aprobarea Compartimentului IT.

2.9. Drepturi de acces

Accesul la sistemele informatice se acordă exclusiv pe baza atribuțiilor de serviciu și a principiului „necesității de a cunoaște”.

Fiecare utilizator:

- utilizează doar contul propriu;
- accesează numai informațiile autorizate;
- nu încercă să depășească nivelul de acces acordat.

2.10. Conturi de utilizator și parole

Este interzisă:

- divulgarea parolelor;
- utilizarea conturilor altor persoane;
- utilizarea conturilor comune, cu excepția situațiilor aprobate explicit.

Parolele trebuie să:

- conțină minimum 12 caractere;
- includă litere mari și mici, cifre și caractere speciale;
- fie schimbate periodic;
- nu conțină date personale ușor identificabile.

2.11. Utilizarea internetului

Accesul la internet se realizează exclusiv prin infrastructura securizată a spitalului.

Compartimentul IT poate restricționa accesul la anumite site-uri sau servicii considerate nesigure ori incompatibile cu activitatea profesională.

Utilizatorii au obligația de a verifica autenticitatea și siguranța informațiilor accesate online.



Spitalul Județean de Urgență
Dr. Constantin Andreoiu Ploiești
Str. Găgeni nr. 100
Tel: +40244537711, Fax: +40244530678
E-mail: secretariat@sjup.ro
Website: www.sjup.ro



2.12. E-mail și comunicare electronică

Utilizarea e-mailului instituțional se realizează exclusiv în interes profesional.

Este interzisă:

- transmiterea de informații confidențiale către destinatari neautorizați;
- distribuirea de materiale ofensatoare, ilegale sau necorespunzătoare;
- utilizarea serviciilor externe neautorizate pentru transferul datelor medicale.

Datele medicale și datele cu caracter personal vor fi transmise numai prin canalele aprobate de spital și cu respectarea prevederilor GDPR.

2.13. Protecția datelor cu caracter personal

Prelucrarea datelor cu caracter personal se realizează cu respectarea:

- Regulamentului (UE) 2016/679 – GDPR;
- Legii nr. 190/2018.

Accesul la datele pacienților este permis numai personalului autorizat și exclusiv în scop profesional.

Orice incident privind securitatea datelor trebuie raportat imediat Responsabilului IT și Responsabilului cu Protecția Datelor (DPO).

2.14. Securitate cibernetică și raportarea incidentelor

Orice utilizator are obligația de a raporta imediat:

- tentative de phishing;
- acces neautorizat;
- pierderea echipamentelor;
- infectări malware;
- divulgarea accidentală de date;
- incidente de securitate cibernetică.

Raportarea se face către Compartimentul IT și DPO.

2.15. Respectarea drepturilor de autor

Este interzisă utilizarea, copierea sau distribuirea neautorizată a programelor software, documentelor sau altor materiale protejate prin drepturi de autor.

3. Dispoziții finale

Nerespectarea prevederilor prezentei politici poate atrage:

- răspundere disciplinară;
- răspundere civilă;
- răspundere contravențională sau penală, după caz.

Prezenta politică intră în vigoare la data aprobării și este obligatorie pentru întreg personalul spitalului.

DPO – Spitalul Județean de Urgență Dr. Constantin Andreoiu Ploiești
Consilier Șerpescu Iulian

Prestator,
SC FAXIMA PRODCOM SRL
Prin reprezentant legal,
Valentin Dumitran

