Spitalul Judetean de Urgenta Targoviste **Aprobat MANAGER**

Str. Tudor Vladimirescu NR. 48 Targoviste **Dr.Petrescu Radu**

Tel 0245611412 ; Fax 0245210509

Nr.Reg………………/…………………..

**Serviciul de Informatică**

**REGULAMENT**

# privind utilizarea şi securitatea Resurselor Informatice şi de Comunicaţii din cadrul reţelei *dbspital* a SJU Targoviste

## **Capitolul 1. INTRODUCERE**

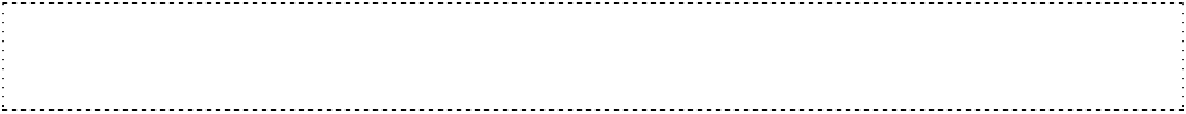
În acord cu prevederile din prezentul regulament, Resursele Informatice şi de Comunicaţii puse la dispozitie şi administrate de către Serviciul de Informatica sunt bunuri strategice ale SJU Targoviste care trebuie administrate ca resurse ale statului român.

Compromiterea securităţii acestor resurse poate afecta capacitatea SJU Targoviste de a oferi servicii informatice şi de comunicaţii, poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilităţii instituţiei în faţa partenerilor săi.

Prin urmare, prezentul regulament este motivat tehnic de necesitatea menţinerii în funcţiune, în condiţii de securitate, a reţelei *dbspital*, precum şi de necesitatea dezvoltării normale a unei resurse de informare.

* 1. **Reţeaua *dbspital***

Reţeaua de calculatoare a SJU Targoviste (numită *dbspital* în cele ce urmează) cuprinde totalitatea Resurselor Informatice şi de Comunicaţie ale SJU Targoviste cu sau fără acces la reţeaua Internet/Intranet.



Reţeaua *dbspital* are ca scop sprijinirea procesului de învăţământ şi cercetare prin mijloacele de comunicare şi serviciile specifice oferite de reţelele de calculatoare conectate în Internet.

Orice activitate care se desfăşoară prin intermediul reţelei *dbspital* trebuie să respecte legislaţia în vigoare (internă şi internaţională): *Legea nr. 64/2004*, *Legea nr. 285/2004*, *Legea nr. 451/2004*, *Legea nr. 496/2004*, *Legea nr. 506/2004*, *Legea nr. 51/2003*, *Legea nr. 161/2003*, *Legea nr. 196/2003*, *Legea 365/2002*, *Legea nr. 455/2001*, *Legea nr. 677/2001*, *Legea nr. 8/1996*, *HG nr. 1308/2002*, *Convenţia privind Criminalitatea Informatică a Consiliului Europei*, *Declaraţia privind libertatea comunicării pe Internet a Consiliului Europei, etc.)*, *regulamentul de funcţionare si organizare* ale SJU Targoviste, precum şi prezentul *Regulament*.Definiţii şi termeni

**Internet =** reţeaua internaţională de calculatoare. Regulile acestei reţele se regăsesc în prevederile InterNIC, RIPE, etc.

**Cont** = o entitate specificată printr-un identificator şi/sau parolă pentru accesul la sistemul de comunicaţie şi/sau la o resursă de calcul.

**Administrator de reţea** = o persoană calificată şi autorizată, responsabilă pentru gestionarea şi operarea unor resurse de calcul şi/sau de comunicaţie pentru uzul altor persoane.

**Resurse Informatice şi de Comunicaţii (RIC)** = toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare, şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: servere, calculatoare personale, calculatoare-agendă (notebookuri, laptop-uri), calculatoare de buzunar, asistent digital personal (Personal Digital Assistant - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), medii de reţea, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.

**Utilizator** = o persoană, o aplicaţie automatizată sau proces utilizator autorizat de către SJU Targoviste şi Medicină Veterinară „Ion Ionescu de la Brad” din Iaşi, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicaţii ale dbspital (a se vedea ).

**Abuz de privilegii** = orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele SJU Targoviste şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.

**Furnizor** = persoană fizică/juridică care oferă bunuri sau servicii SJU Targoviste în baza unui contract comercial sau de colaborare.

## **Capitolul 2. POLITICA DE SECURITATE**

Politica de securitate este alcătuită astfel încât să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice publice, să stabilească practici prudente şi acceptabile privind utilizarea Resursele Informatice şi de Comunicaţii ale SJU Targoviste şi să instruiască utilizatorii care au dreptul de folosire a Resurselor Informatice şi de Comunicaţii privind responsabilităţile asociate unei astfel de utilizări.

### Audienţă

Politica de securitate a Resurselor Informatice şi de Comunicaţii ale SJU Targoviste se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice RIC a instituţiei. Nu există niciun fel conotaţii politice, religioase, rasiale legate de prevederile politicii de securitate. Trebuie privită doar ca un instrument de protecţie a datelor din sistemul informatic şi nu ca un element restrictiv.

sau alte persoane, entităţi şi organizaţii care au acces la Resursele Informatice şi de Comunicaţii ale SJU Targoviste .

### Scop

Scopul urmărit de politica de securitate este acela de asigurare a integrităţii, confidenţialităţii şi disponibilităţii informaţiei, precum şi stabilirea cadrului necesar pentru elaborarea regulilor şi procedurilor de securitate

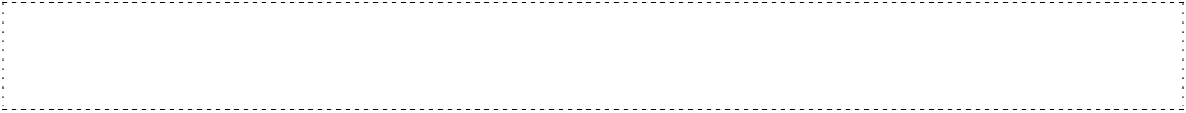
*Confidenţialitatea* se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul SJU Targoviste sunt proprietatea SJU Targoviste în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la Resursele Informatice şi de Comunicaţii.

*Integritatea* se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate.

*Disponibilitatea* se asigură prin funcţionarea continuă a tuturor componentelor Resurselor Informatice şi de Comunicaţii. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a Resurselor Informatice şi de Comunicaţii.

### Clasificarea informaţiilor

Clasificarea informaţiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora, cât şi pentru a determina pierderile potenţiale ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.



Pentru a asigura securitatea şi integritatea informaţiilor, acestea se împart în trei categorii principale: publice, secrete şi strict secrete.

**Publice:** Acestea sunt informaţiile accesibile oricărui utilizator din interiorul sau exteriorul SJU Targoviste . Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra instituţiei sau aceste efecte sunt nesemnificative. Utilizatorii care furnizează aceste informaţii sunt responsabili de asigurarea integrităţii şi disponibilităţii acestora în raport cu cerinţele SJU Targoviste .

*Exemple*: Informaţiile de pe aviziere, servere web publice, ştirile de presă, anunturile publice.

**Secrete:** În această categorie se includ informaţiile care datorită valorii economice nu trebuie făcute publice. Se includ aici şi informaţiile pe care SJU Targoviste trebuie să le protejeze conform legislaţiei în vigoare. Datorită valorii economice asociate, aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate şi distribuite în cadrul SJU Targoviste doar utilizatorilor autorizaţi. Distribuirea acestor informaţii de către utilizatorii autorizaţi trebuie să se facă pe baza unei clauze de confidenţialitate.

*Exemple*: clauze contractuale, conturi si parole folosite pe serverele sistemului informatic.**Strict Secrete sau Confidenţiale:** În această categorie se includ toate informaţiile care datorită valorii economice nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidenţa Codului Civil, Penal sau legislaţiei fiscale. Accesul la aceste informaţii va fi restricţionat. Datele strict secrete nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii SJU Targoviste.

*Exemple*: cheile criptografice, conturi administrative de pe serverele de gestiune a sistemului informatic.

### Atribuţii şi responsabilităţi

#### Atribuţii manageriale

Orice angajat sau compartiment al SJU Targoviste

trebuie să se asigure că managementul respectă prevederile prezentei Politici şi a regulamentelor sau procedurilor asociate.

Administratorii de reţea/sistem/baze de date trebuie să asigure existenţa jurnalelor şi a traseelor auditării pentru orice tip de acces în sistem conform regulilor sau procedurilor asociate.

Administratorii de reţea/sistem/baze de date trebuie să asigure activarea tuturor mecanismelor de securitate.

Compartimentul de audit intern este responsabil de evaluarea schemei de clasificare a informaţiilor.

#### Atribuţii şi obligaţii ale administratorilor reţelei *dbspital*

Administratorul reţelei *dbspital* este Serviciul de Informatica, structură creată prin decizie a Conducerii SJU Targoviste. Desemnarea *Serviciului de Informatica* ca administrator are ca scop stabilirea în mod clar a responsabilităţii privind administrarea şi buna funcţionare a Resurselor Informatice şi de Comunicaţii din cadrul reţelei *dbspital*, precum şi a responsabilităţii privind crearea, modificarea şi aprobarea regulilor şi politicilor referitoare la activităţile de administrare şi utilizare a Resurselor Informatice şi de Comunicaţii.

Atribuţiile şi obligaţiile Serviciului de Informatica includ:

* Elaborarea şi propunerea de modificări ale politicii de securitate a sistemului RIC ;
* Elaborarea şi propunerea pentru aprobare a planului de securitate (acesta conţine o listă a tuturor regulilor şi procedurilor de securitate aplicabilela sistemul de RIC ;
* Elaborarea procedurilor pentru identificarea utilizatorilor RIC ;
* Tratarea incidentelor de securitate în scopul minimizării efectului distructiv al acestora asupra RIC.
* Facilitarea evaluărilor legale, a cerinţelor de tip „cele mai bune practici" pe măsură ce acestea devin recunoscute.

#### Atribuţii şi obligaţii ale utilizatorilor reţelei *dbspital*

Utilizatorii reţelei *dbspital* pot fi sunt reprezentaţi de: cadre medicale, personal administrativ, alti angajati ai SJU Targoviste care solicită calitatea de utilizator.

Alte categorii cum ar fi: furnizori de servicii sau reprezentanti ai altor instituţii etc., pot deveni utilizatori ai *dbspital* în baza unei cereri motivate avizate de Serv. Informatica si aprobate de conducerea SJU Targoviste . Deasemnea utilizatorul este obligat sa semneze un acord de confidentialitate.

Utilizatorii standard nu au drept de administrare a reţelei şi pot folosi numai acele RIC pentru care sunt autorizaţi, indiferent dacă sunt resurse locale sau resurse accesibile în Internet. Atribuţiile şi obligaţiile utilizatorilor sunt următoarele:

* Să cunoască şi să respecte prevederile politicii de securitate a RIC ;
* Să cunoască şi să respecte prevederile tuturor regulilor şi procedurilor privind securitatea RIC (***vezi Anexe*);**
* Să răspundă direct de securitatea şi conţinutul informaţiilor şi resursele informatice şi de comunicaţii încredinţate direct sau indirect.

#### Alte atribuţii

Toţi partenerii SJU Targoviste (furnizori, agenţi, colaboratori etc.) trebuie să accepte şi să respecte politica de securitate, precum şi regulile specifice privind utilizarea şi securitatea Resurselor Informatice şi de Comunicaţii ale *dbspital*.

### Prevederi pentru asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei în utilizarea Resursele Informatice şi de Comunicaţii ale SJU Targoviste

Politica de securitate a SJU Targoviste impune dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau reguli specifice care să asigure integritatea, confidențialitatea și disponibilitatea informației în utilizarea RIC. Toate procedurile şi/sau regulile aplicabile în sistemul Resurselor Informatice şi de Comunicaţii ale *dbspital* fac parte din Planul de Securitate (*vezi capitolul 3*) şi sunt obligatorii pentru toţi utilizatorii.

Se recomandă ca prevederile politicii de securitate să fie incluse în contractul de muncă şi toate contractele cu terţi (dacă activitatea acestora are legătură cu sistemul Informatic şi de Comunicaţii al SJU Targoviste).

Întreg personalul este responsabil privind modul de utilizare a RIC şi nu trebuie să facă abuz de privilegii; fiecare utilizator este direct responsabil pentru acţiunile care pot afecta securitatea Resurselor Informatice şi de Comunicaţii.

Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a politicii de securitate.

Nu există nicio asigurare a confidenţialităţii datelor personale sau a accesului la informaţii folosind protocoale de genul, dar nu numai, mesagerie electronică, navigare Web, conversaţii telefonice, transmisie fax-uri şi alte instrumente de conversaţie electronică. Utilizarea acestor instrumente de comunicaţie electronică poate fi monitorizată în scopul unor investigaţii sau al rezolvării unor plângeri în condiţiile legilor în vigoare.

Departamentele şi Sectiile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC.

Orice informaţie folosită în sistemul RIC trebuie să fie păstrată confidenţială şi în siguranţă de către utilizator. Faptul că informaţiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidenţiale şi în siguranţă, tipul informaţiei sau chiar informaţia în sine stau la baza determinării gradului de siguranţă necesar.

Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele sunt proprietatea SJU Targoviste şi trebuie să fie protejate.

Departamentele şi Sectiile trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIC, protejării datelor şi programelor împotriva întrebuinţării greşite, în concordanţă cu necesităţile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător. Orice program comercial utilizat în cadrul RIC trebuie să fie însoţit de Licenţă care să specifice clar drepturile de utilizare şi restricţiile produsului. Personalul trebuie să respecte prevederile Licenţelor si nu este permisă copierea ilegală a programelor comerciale. Serviciul de Informatica, direct sau prin intermediul Departamentelor şi Sectiilor, îşi rezervă dreptul de a şterge orice produs fără licenţă de pe orice sistem din cadrul Resurselor Informatice şi de Comunicaţii.

Serviciul de Informatica, direct sau prin intermediul Departamentelor şi Sectiilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective.

Domeniul electronic  *spitaldb.ro* şi subdomeniile acestuia sunt gestionate de SJU Targoviste ca domenii proprii, în conformitate cu înregistrarea corespunzătoare a SJU Targoviste ca proprietar al acestui domeniu la autoritatea românească în materie de nume de domenii (RNC). Drepturile de utilizare ale domeniului  *spitaldb.ro* sunt rezervate pentru SJU Targoviste. Informaţiile publicate electronic de către SJU Targoviste pe site-ul propriu [*www.spitaldb.ro*](http://www.spitaldb.ro)şi în subdomeniile acestuia sunt proprietate a SJU Targoviste. Caracterul public al acestora reflectă faptul că ele sunt puse la dispoziţie de către SJU Targoviste în beneficiul comunităţii publice, în scop de informare asupra programelor academice şi a activităţii SJU Targoviste.

Informaţiile depuse pe site-urile publice ale SJU Targoviste aparţin SJU Targoviste. Orice utilizare a informaţiilor de pe site-urile publice ale SJU Targoviste în domeniul  *spitaldb.ro* de către persoane particulare sau organizaţii în alte scopuri decât cele în care au fost oferite, se face pe propria răspundere a acestora. Într-o asemenea eventualitate, SJU Targoviste îşi rezervă dreptul de a solicita aplicarea prevederilor legale în vigoare.

Fişierele electronice create, trimise, primite sau stocate folosind Resursele Informatice şi de Comunicaţii administrate sau în custodia şi sub controlul SJU Targoviste nu au caracter personal şi pot fi accesate oricând de către angajaţii autorizaţi din cadrul Serviciului de Informatica, Departamente şi Sectii fără înştiinţarea utilizatorului.

În scopul administrării RIC şi pentru asigurarea securităţii acestora, personalul autorizat poate revizui sau utiliza orice informaţie stocată pe sau transportată prin sistemele Resurselor Informatice şi de Comunicaţii în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor (de exemplu: pagini web vizitate).

Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul SJU Targoviste , orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea Serviciului de Informatica).

Un mare număr de utilizatori, pot accesa informaţii din exteriorul sistemului de comunicaţii al SJU Targoviste . În aceste condiţii este obligatorie păstrarea confidenţialităţii informaţiilor transmise din exteriorul SJU Targoviste şi a informaţiilor obţinute din interiorul institiţiei.

Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele SJU Targoviste pentru care nu au autorizaţie sau consimţământ explicit.

Niciun utilizator al Resurselor Informatice şi de Comunicaţii SJU Targoviste nu poate divulga informaţiile la care are acces

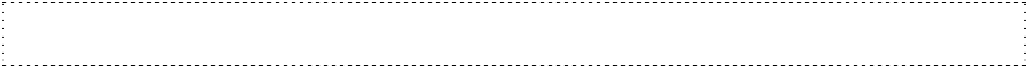
sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemelor ce compun Resursele Informatice şi de Comunicaţii. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu SJU Targoviste .

Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicaţii ale terţilor nu poate fi asigurată. Pentru aceste situaţii, confidenţialitatea şi integritatea informaţiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligaţi să se asigure că toate informaţiile confidenţiale ale SJU Targoviste se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

## **Capitolul 3. PLANUL DE SECURITATE**

### Introducere

Planul de securitate conţine toate regulile şi procedurile aplicabile în sistemul Resurselor Informatice şi de Comunicaţii a *dbspital*.



Acestea sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în SJU Targoviste .

### Scop

În acord cu legislaţia în vigoare în România şi Regulamentele de ordine interioară ale SJU Targoviste , Resursele Informatice şi de Comunicaţii sunt valori ale SJU Targoviste care trebuie exploatate şi administrate ca resurse publice în proprietatea statului român.

Planul de securitate are ca scop principal protejarea utilizatorilor şi colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea, acesta are ca scop protejarea imaginii SJU Targoviste şi a investiţiilor acesteia pentru dezvoltarea sistemului informatic şi de comunicaţii, protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate cu ajutorul Resurselor Informatice şi de Comunicaţii ale utilizatorilor autorizaţi: cadre medicale, personal administrativ, colaboratori etc.

Regulile (***vezi anexele prezentului Regulament***) au fost elaborate pentru fiecare activitate specifică domeniului şi au fost concepute în aşa fel încât fiecare să poată fi folosită cvasi- independent de celelalte

Regulile şi procedurile din planul de securitate au rolul:

* de a fi corecte, echitabile şi eficiente pentru folosirea RIC în vederea sprijinirii procesului educaţional şi al cercetării ştiinţifice.
* de a educa utilizatorii RIC în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora.
* de a fi compatibile cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

### Audienţă

Regulile de utilizare a Resurselor Informatice şi de Comunicaţii ale SJU Targoviste se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acestea.

### Proceduri şi Reguli specifice

Aceasta este lista tuturor regulilor sau procedurilor aplicabile în sistemul Resurselor Informatice şi de Comunicaţii:

1. Reguli de Utilizare a Resurselor Informatice şi de Comunicaţii (Anexa 1)
2. Reguli privind accesul fizic la Resursele Informatice şi de Comunicaţii (Anexa 2)
3. Reguli de acces la reţeaua de comunicaţii (Anexa 3)
4. Reguli de acces administrativ (*Anexa 4*)
5. Reguli privind configurarea sistemelor informatice pentru acces la reţeaua de comunicaţii (*Anexa 5*)
6. Reguli de tratare a incidentelor de securitate (*Anexa 6*)
7. Reguli de monitorizare a Resurselor Informatice şi de Comunicaţii (*Anexa 7*)
8. Reguli pentru detectarea accesului neautorizat (*Anexa 8*)
9. Reguli privind crearea şi utilizarea copiilor de siguranţă (*backup*) (*Anexa 9*)
10. Reguli de securizare a serverelor (*Anexa 10*)
11. Reguli privind securitatea informaţiilor în cazul utilizării calculatoarelor portabile (*Anexa 11*)
12. Reguli pentru parolele de acces (*Anexa 12*)
13. Reguli de administrare a conturilor de email (*Anexa 13*)
14. Reguli privind sistemul de mesagerie electronică (*Anexa 14*)
15. Reguli de detectare a viruşilor (*Anexa 15*)
16. Reguli de relaţii cu terţi (*Anexa 16*)
17. Reguli pentru modificări şi modernizări ale RIC (*Anexa 17*)
18. Procedură pentru alocarea unei adrese de email. Cerere tip (*Anexa 18*)
19. Procedură pentru conectarea la reţea. Cerere tip (*Anexa 19*)
20. Proces verbal de constatare (*Anexa 20*)
21. Exemple de activităţi interzise (*Anexa 21*)

## **Capitolul 4. MĂSURI DISCIPLINARE**

Administratorul reţelei *dbspital* are dreptul să ia măsuri de restricţionare (blocare parţială sau totală), fără notificare, a accesului la Resursele Informatice şi de Comunicaţii în cazul utilizatorilor care încalcă prevederile politicii de securitate şi regulile aplicabile în sistemul de RIC (din planul de securitate) sau legislaţia în vigoare şi care, astfel, pun în pericol funcţionarea şi/sau securitatea reţelei *dbspital*.

În situaţii cu totul deosebite, când eventuale acţiuni ale unor utilizatori care, pe proprie răspundere, atentează grav la securitatea reţelei *dbspital*, se pot lua următoarele măsuri:

* rezilierea contractului de muncă în cazul angajaţilor;
* încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, furnizorilor sau consultanţilor; Toate acţiunile care contravin legilor vor fi raportate organelor competente.

## 

## **Capitolul 5. REFERINŢE**

* Politica şi Planul de securitate ale UAIC;
* RFC 1244 – Site Security Handbook: [www.ietf.org/rfc/rfc1244.txt](http://www.ietf.org/rfc/rfc1244.txt) ;
* *Legea nr. 676* din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor;
* *Legea nr. 455* din 18 iulie 2001 privind semnătura electronică;
* *Legea nr. 544* din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
* *Hotărârea nr. 1259* din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea *Legii nr. 455* din 2001 privind semnătura electronică;
* *Ordinul nr. 52* din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal;
* *Ordinul nr. 53* din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
* *Hotărârea nr. 781* din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu;
* *Legea nr. 182* din 12 aprilie 2002 privind protecţia informaţiilor clasificate;
* *Legea nr. 161* din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei.

## **Capitolul 6. DISPOZIŢII FINALE**

Regulamentul va fi disponibil în format electronic pe site-ul web al SJU Targoviste . Se recomandă ca acest document să fie disponibil sau să se facă trimitere la acesta de pe toate site-ul web din cadrul SJU Targoviste.

Prezentul document va conţine informaţii de identificare proprii şi se va specifica data la care a fost aprobat şi data de la care intră în vigoare.

Modificarea prevederilor Regulamentului se face numai cu aprobarea conducerii SJU Targoviste . Fiecare modificare a conţinutului va conduce la modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune intră în vigoare.

#### Prezentul Regulament a fost supus spre aprobare, discutat şi aprobat în ședința Conducerii SJU Targoviste din ………………………… şi va intra în vigoare de la data de …………………….