

Nr. 4466 din 18.03.2021

Revizie 1

**Regulament privind utilizarea
Rețelei Informaticice și de Comunicații a
Spitalului Orășenesc ‘Sfântul Dimitrie’ Târgu Neamț**

I. Rețeaua de calculatoare

Art. 1. Rețeaua Informatică și de Comunicații a Spitalului Orășenesc ‘Sfântul Dimitrie’ –Târgu Neamț, denumita în continuare RICSOTGNT cuprinde totalitatea echipamentelor de calcul și comunicație.

Art. 2. RICSOTGNT are ca scop sprijinirea procesului stocare, informare, prelucrarea a datelor prin mijloacele de comunicație și serviciile informaticice de rețeaua de calculatoare conectata la rețea RICSOTGNT.

Art. 3. Orice activitate care se desfășoară prin intermediul Retelei de calculatoare RICSOTGNT trebuie să respecte legislația internă și internațională

Legea nr. 64/2004 privind ratificarea Convenției Consiliului Europei privind criminalitatea informatică

Legea 8/1996, Legea nr. 285/2004 și Legea nr. 329/2006 privind drepturi de autor și drepturi conexe,

Legea nr. 196/2003, Legea 496/2004 privind prevenirea și combaterea pornografiai

Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal, Legea nr. 455/2001 –privind semnatura electronică

Legea nr. 679/2018 –privind protecția datelor cu caracter personal

Legea nr. 362/2018 -privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatic

Art. 4. Administratorul RICSOTGNT este Serviciul de Informatică Evaluare Statistică Medicală denumit SIESM, structura creata prin organograma spitalului și are ca sarcini:

1. asigurarea funcționării în bune condiții a RICSOTGNT;
2. planificarea și coordonarea dezvoltării RICSOTGNT;
3. acordarea de asistență tehnică de specialitate utilizatorilor;
4. stabilirea regulilor și politicilor de utilizare a RICSOTGNT;
5. administrarea propriu-zisă.

Art. 5. Prezentul regulament este elaborat de către SIESM și este motivat strict tehnic de necesitatea menținerii în funcțiune în condiții de siguranță și de necesitatea unei dezvoltări normale a unei resurse informaționale, considerată de Spitalul Orășenesc ‘Sfântul Dimitrie’ Tîrgu Neamț ca obiectiv strategic. El trebuie privit ca un instrument de protecție a muncii utilizatorilor, și nu ca un element restrictiv.

II.Definiții și termeni utilizati

Art. 6. Internet este rețeaua internațională de calculatoare. Regulile acestei rețele se regăsesc în prevederile INTERNIC, RIPE, etc.

Art. 7. Resursă de calcul este orice obiect (fizic sau logic) cu care se poate realiza o procesare a informației (indiferent de natura acesteia). Exemple de resurse de calcul (fără a se limita însă numai la acestea) sunt: calculatoarele individuale, serverele de rețea ,laptopuri de serviciu.

Art. 8. Sistemul de comunicație format din resurse de comunicație reprezintă partea logică și fizică care face posibil schimbul de informații între resursele de calcul. Exemple de resurse de comunicație (fără a se limita însă numai la acestea) sunt: routerele, switchurile, modemurile, huburile, elementele de legătură.

Art. 9. Cont este o entitate specificată printr-un identificator și/sau parolă pentru accesul la sistemul de comunicație și/sau la o resursă de calcul.

Art. 10. Utilizator este orice persoană ce folosește RICSOTGNT.

Art. 11. Administrator de rețea este o persoană calificată și autorizată, responsabilă pentru gestionarea și operarea unor resurse de calcul și/sau de comunicație pentru uzul altor persoane.

Art. 12. Administrator Web este o persoană calificată și autorizată, responsabilă pentru gestionarea și operarea unor resurse și informații care formează un site Web ,intranet .

III. Drepturile și obligațiile administratorilor și utilizatorilor RICSOTGNT.

Art. 13. Administratorul RICSOTGNT va răspunde de buna funcționare a resursei/resurselor pe care le are în administrare și de stabilirea regulilor de utilizare a acestora.

Art. 14. Administratorul are obligația de a-și perfecționa în mod constant pregătirea profesională.

Art. 15. Administratorul, fiind automat și utilizator, trebuie să respecte secțiunea referitoare la utilizatorii RICSOTGNT.

Art. 16. Având drepturi sporite față de utilizatorii obișnuiți, administratorii nu trebuie să abuzeze de acestea.

Art. 17. Administratorul va controla periodic starea resurselor pe care le are în administrare și va semnala celor abilități disfuncționalitățile apărute.

Art. 18. Administratorul ia măsuri pentru descoperirea oricărei utilizări neautorizate sau ilegale a resurselor pe care le administrează, precum și a autorilor acestor abuzuri.

Art. 19. Administratorul are dreptul să ia măsuri de restricționare fără notificare a accesului la RICSOTGNT asupra utilizatorilor care încalcă prezentul regulament sau legislația în vigoare, atunci când situația o impune – continuarea activității acestor utilizatori pune în pericol funcționarea și/sau securitatea RICSOTGNT.

Art. 20. În cazul în care un administrator încalcă acest regulament el va fi avertizat.

Dacă abaterea se repetă el va fi sancționat prin retragerea calității de administrator.

IV. Utilizatorii Retelei de calculatoare RICSOTGNT

Art. 21. Utilizatorii RICSOTGNT sunt:

1. personal conducere;
2. personal contabil;
3. personal resurse umane;
4. personal achiziții
5. personal administrativ;
6. personal medical;
7. colaboratori, care solicită calitatea de utilizator.

Se recomandă ca prevederile politicii de securitate să fie incluse în contractul de muncă și în toate contractele cu terți - dacă activitatea acestora are legătura cu sistemul informatic și de comunicații al unității.

Politica de securitate va fi aplicată fiecărui salariat în funcție de locul de muncă și responsabilitățile individuale.

Fiecare salariat va primi un identificator unic de utilizare al RICSOTGNT ,care va permite accesul diferențiat la aplicații și resurse.

Fiecare salariat va avea acces doar la informațiile specifice locului de muncă (secție medicală , serviciu, birou , compartiment , cabinet) , conform organigramei și răspunderii specifice .

Modificarea , alterarea , ștergerea datelor vor fi restricționate doar pentru utilizatorii care au acest drept ,iar operațiunile vor fi jurnalizate .

Identificatorul unic al salariatului (user și parolă) nu va permite accesul la informații care nu sunt specifice locului de muncă al salariatului sau la care acesta nu trebuie să aibă acces.

Personalul de conducere va avea acces în:

- aplicații medicale (Infoworld, PACS)
- aplicații financiar-contabile
- aplicații resurse umane
- aplicații statistice
- aplicații de laborator
- aplicații pentru serviciul achiziții
- aplicații de farmacie
- aplicații juridice
- mail de serviciu
- intranet

Personalul medical-medici va avea acces în:

- aplicații medicale (Infoworld, PACS)
- aplicații resurse umane (pontaje,grafice de lucru)
- aplicații financiar-contabile(referate , stocuri)
- aplicații statistice
- aplicații pentru serviciul achiziții
- aplicații de laborator
- aplicații de farmacie
- mail de serviciu
- intranet

Personalul medical-asistenți medicali va avea acces în:

- aplicații medicale (Infoworld, PACS)
- aplicații resurse umane (pontaje,grafice de lucru)
- aplicații financiar-contabile(referate , stocuri)
- aplicații statistice
- aplicații pentru serviciul achiziții
- aplicații de laborator
- aplicații de farmacie
- mail de serviciu
- intranet

Personalul medical-registratori medicali va avea acces în:

- aplicații medicale (Infoworld, PACS)
- aplicații resurse umane (pontaje,grafice de lucru)
- aplicații financiar-contabile(referate , stocuri)
- aplicații statistice
- aplicații de laborator

- aplicații de farmacie
- mail de serviciu
- intranet

Personalul TESA-RUONS va avea acces în:

- aplicațiile resurse umane
- aplicațiile finanțări-contabile
- aplicațiile statistice
- aplicații juridice
- mail de serviciu
- intranet

Personalul TESA- finanțări-contabil va avea acces în:

- aplicațiile resurse umane
- aplicațiile finanțări-contabile
- aplicațiile statistice
- mail de serviciu
- intranet

Personalul TESA- achiziții va avea acces în:

- aplicațiile finanțări-contabile
- aplicațiile de achiziții
- mail de serviciu
- intranet

Personalul TESA-SIESM va avea acces în:

- aplicațiile medicale (Infoworld, PACS)
- aplicațiile finanțări-contabile
- aplicațiile resurse umane
- aplicațiile statistice
- aplicații de laborator
- aplicații pentru serviciul achiziții
- aplicații de farmacie
- aplicații juridice
- mail de serviciu
- intranet

Personalul TESA-Birou Tehnic Administrativ va avea acces în:

- aplicațiile finanțări-contabile
- aplicații pentru serviciul achiziții
- aplicații juridice
- mail de serviciu
- intranet

Personalul TESA-Arhiva va avea acces în:

- aplicații pentru serviciul achiziții
- aplicații juridice
- mail de serviciu
- intranet

Personalul TESA-SSM/PSI va avea acces în:

- aplicații pentru serviciul achiziții
- aplicații juridice
- mail de serviciu
- intranet

Personalul TESA-MCSS va avea acces în:

- aplicațiile statistice

- aplicații juridice
- mail de serviciu
- intranet

Personalul Ambulatoriu-fișier va avea acces în:

- aplicațiile finanțier-contabile
- mail de serviciu
- intranet

Art. 22. Pot deveni utilizatori ai RICSOTGNT, în baza unei cereri motivate și a unei recomandări din partea unui membru al conducerii, în general personalul nou angajat.

Art. 23. Se consideră a priori că toți utilizatorii sunt de bună credință și comportamentul lor este corespunzător unor standarde ridicate de morală și etică.

Următoarele principii stabilesc regulile de conduită pentru utilizatorii RICSOTGNT.

Art. 24. Utilizatorii au obligația de a citi și a cunoaște prevederile acestui regulament. Neștiința și ignoranța nu pot fi folosite drept scuză pentru cauzarea de disfuncționalități ale RICSOTGNT sau încălcări ale regulamentului sau ale legislației în vigoare.

Art. 25. Utilizatorii poartă întreaga responsabilitate pentru acțiunile executate nemijlocit din conturile pe care le au la RICSOTGNT, precum și de pe resursele de calcul/comunicație pe care le folosesc.

Art. 26. Resursele și serviciile RICSOTGNT vor fi folosite în mod responsabil, etic, în spirit deschis și cu respectarea legislației în vigoare.

Art. 27. Utilizatorii vor folosi numai acele resurse pe care sunt autorizați să le folosească, indiferent dacă sunt resurse ale RICSOTGNT sau resurse accesibile în Internet.

Art. 28. Utilizatorii vor lua toate măsurile rezonabile pentru a asigura integritatea și confidențialitatea resurselor hardware și software din RICSOTGNT. În particular, utilizatorii:

1. nu vor divulga altor persoane parolele/mecanismele de acces și nu vor oferi drept de folosire a conturilor proprii;
2. vor păstra secretul parolelor;
3. nu vor face publice informații legate de structura și organizarea RICSOTGNT.

Art. 29. Utilizatorii se obligă să asigure securitatea RICSOTGNT. Serviciul SIESM nu își asumă responsabilitatea în cazul apariției oricărora probleme de securitate în acele subsisteme ale RICSOTGNT aflate în administrarea utilizatorilor (rețele locale ale utilizatorilor, etc.), obligația de a-și asigura securitatea aparținând în exclusivitate acestora.

Art. 30. Utilizatorii vor folosi în RICSOTGNT date și software numai în condițiile respectării legilor privind dreptul de autor și licențiere ale posesorilor acestora.

Art. 31. Utilizatorii vor respecta regulile stabilite de administratorii altor rețele externe, atunci când accesează resursele acestora, precum și regulile stabilite prin prezentul regulament și de legislația în vigoare.

Art. 32. Utilizatorii vor respecta caracterul personal al datelor și resurselor de calcul/comunicație aparținând celorlalți utilizatori.

Art. 33. Datele transmise și stocate în RICSOTGNT trebuie să fie informații motivate de interesul utilizatorilor, interes care nu poate presupune:

1. generare de trafic personal;
2. perturbară a traficului RICSOTGNT;
3. promovare de activități comerciale neautorizate;
4. generare de trafic excesiv, care împiedică funcționarea rețelei în condiții normale;
5. transferuri de materiale pornografice;

6. transferuri de materiale care contravin legilor drepturilor de autor (software piratat, filme, muzică, etc.);
7. tentative de exploatare a problemelor de securitate care pot apărea (accesul, alterarea sau stergerea neautorizată a datelor sau software-ului, răspândirea de aplicații informaticе din categoria software-ului malicioș: virusi, troieni, viermi, spyware, etc.);
8. distrugerea sau încercarea de a distrage securitatea RICSOTGNT;
9. compromiterea sau tentativa de compromitere a integrității resurselor de calcul/comunicație;
10. hărțuirea altor utilizatori;
11. utilizarea resurselor, în particular poștă electronică, servere de Web și buletine, pentru a transmite mesaje obscene, repetitive, frauduloase sau nesolicitante, cu caracter comercial (de exemplu, spam).
12. utilizarea de software fără a cunoaște efectele pe care acesta le produce;

Art. 34. Utilizatorii sunt obligați să trateze RICSOTGNT ca pe o resursă comună, care trebuie să fie protejată și să semnaleze la SIESM orice intruziune străină în rețea sau operațiune din clasa descrisă anterior (în Art. 33).

Art. 35. Este interzisă adăugarea, modificarea sau scoaterea de resurse în sau din RICSOTGNT fără acordul SIESM își rezervă dreptul de a anula modificările făcute fără acordul său.

Art. 36. RICSOTGNT se declară a fi un mediu de lucru și comunicare deschis. Utilizatorii sunt invitați să se trateze reciproc în mod politic și cordial. Partenerii noștri din Internet se așteaptă să găsească în Spitalul Orășenesc ‘Sfântul Dimitrie’ Tg Neamț un mediu academic atunci când solicită informații, motiv pentru care utilizatorii vor lua măsuri pentru a se autoidentifica corect atât în cadrul RICSOTGNT, cât și în corespondență electronică pe care o trimit.

Art. 37. Utilizatorii RICSOTGNT au dreptul la confidențialitate asupra corespondenței și datelor pe care le dețin în resursele din RICSOTGNT. Totuși, ei trebuie să accepte un grad rezonabil de asigurare a acestui drept. Penele de sistem hardware și/sau software, defecțiunile de proiectare a instrumentelor folosite pot duce la căderea sistemelor de securitate și neasigurarea temporară a caracterului confidențial al datelor sau chiar la distrugerea unor informații. În plus, utilizatorii trebuie să accepte dreptul administratorilor RICSOTGNT de a accesa informațiile personale, și anume doar în situațiile în care accesul respectiv este justificat de necesitatea administrației rețelei, și/sau în scopul verificării respectării regulilor stabilite prin acest regulament, precum și prin legislația în vigoare.

Art. 38. Regulile de conduită stabilite de prezentul regulament sunt acceptate liber, prin consimțământ scris, de către fiecare utilizator în parte, în momentul dobândirii calității de utilizator. Nerespectarea lor ulterioară atrage după sine pierderea fără o notificare prealabilă a calității de utilizator și, în funcție de caz, răspunderile civile și/sau penale corespunzătoare legislației în vigoare.

Art. 39. Pe măsura dezvoltării RICSOTGNT pot apărea probleme specifice noi și pot fi necesare completări, modificări ale acestui regulament. SIESM își rezervă dreptul de modificare a regulamentului cu aprobarea conducerii Spitalului Orășenesc “Sf.Dimitrie” Tîrgu Neamț , iar orice modificare a regulamentului va fi adusă la cunoștința utili zatorilor și va fi publicată pe site-ul Web spitalului și pe intranet..



Vizat,
Şef SIESM
Ing. Ceberă Elena

Întocmit,
SIESM
Ing. Ceberă Cătălin

Reguli specifice de utilizare a RICSOTGNT:

- Anexa 1 Reguli de utilizare a Resurselor RICSOTGNT
- Anexa 2 Reguli privind accesul fizic la RICSOTGNT
- Anexa 3 Reguli de acces la rețeaua de comunicații a Spitalului
- Anexa 4 Reguli privind configurarea sistemelor informative pentru acces la rețeaua de comunicatii
- Anexa 5 Reguli de tratare a incidentelor de securitate
- Anexa 6 Reguli de monitorizare a RICSOTGNT
- Anexa 7 Reguli pentru detectarea accesului neautorizat
- Anexa 8 Reguli privind crearea și utilizarea copiilor de siguranță (*backup*)
- Anexa 9 Reguli privind securitatea informațiilor în cazul utilizării calculatoarelor/dispozitivelor portabile
- Anexa 10 Reguli de administrare a conturilor de email
- Anexa 11 Reguli privind sistemul de mesagerie electronică
- Anexa 12 Reguli de detectare a virușilor
- Anexa 13 Reguli de relații cu terții

Anexa 1

REGULI DE UTILIZARE A RESURSELOR INFORMATICE ȘI DE COMUNICAȚII

A.Utilizarea permanentă a resurselor informative și de comunicații

1. Utilizarea RICSOTGNT se face numai în interes de serviciu.
2. Utilizatorii trebuie să anunte despre orice problemă în sistemul de securitate din cadrul Spitalului, cat și despre orice posibila întrebuitare greșită sau încalcare a reglementelor în vigoare.
3. Prin acțiunile lor, utilizatorii nu trebuie să incerce să compromita protecția sistemelor informative și de comunicații și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip.
4. Utilizatorii nu trebuie să încearcă să obțină acces la date sau programe din RICSOTGNT pentru care nu au autorizație sau consimțământ explicit.
5. Utilizatorii nu trebuie să divulge sau să înstrâneze nume de cont-uri, parole , Numere de Identificare Personală(PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau ori ce dispozitive și/sau informații similare utilizate în scopuri de autorizare și identificare.
6. Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală și a dreptului de autor(copyright).
7. Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobare.
8. Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane; să degradeze performanțele sistemelor ce alcătuiesc RICSOTGNT; să împiedice accesul unui utilizator autorizat la RICSOTGNT; să obțină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente.
9. Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității sistemelor ce alcătuiesc RICSOTGNT. De exemplu, utilizatorii nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.
10. RICSOTGNT nu trebuie să fie folosit pentru beneficiul personal.
Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Spitalul le poate considera ofensive, indecente sau obscene.
11. Accesul la rețeaua Internet prin intermediul RICSOTGNT se supune acelorași regulamente care

se aplica utilizării din interiorul institutiei și Regulamentului pentru Utilizare Internet și Intranet.

12. Angajatii nu trebuie să permita membrilor familiei sau altor persoane accesul la RICSOTGNT .

13. Utilizatorii care au acces la RICSOTGNT au obligatia de a purta acte și sau legitimatii care să ateste calitatea de utilizator autorizat în spatiile institutiei.

14. Utilizatorii vor folosi, exclusiv, numele de domeniu în toate activitățile desfășurate prin intermediul sau folosind RICSOTGNT .

15. Utilizatorii nu trebuie să se angajeze în actiuni împotriva scopurilor Spitalului folosind RICSOTGNT.

16. Nu este permisă trimitera sau receptionarea documentelor sau fișierelor care pot cauza actiuni legale împotriva Spitalului sau prejudicierea, indiferent de forma, a intereselor acestuia.

17. Toate mesajele, fisierele si documentele localizate în cadrul RICSOTGNT sunt proprietatea Spitalului și pot fi subiectul unor cereri de verificare /inspectare la accesare conform reglementelor.

B. Utilizarea ocazională a Resurselor Informatice și de Comunicatii

În anumite situații este permisă utilizarea ocazională a RICSOTGNT. În aceste situații se aplică urmatoarele restricții:

-utilizarea personală ocazională a serviciilor de poștă electronică, acces Internet, telefoane, fax-uri, imprimante, copiatoare, etc este restrictionata la utilizatorii autorizati și nu poate fi extinsă la membrii familiilor sau alte persoane;

-utilizarea ocazională a RICSOTGNT nu trebuie să aibă drept rezultate costuri directe pentru Spital; utilizarea ocazională a RICSOTGNT nu trebuie să afecteze activitatea angajatilor

Anexa 2

Reguli privind accesul fizic la Resursele Informatice și de Comunicații

1.Toate sistemele securitate fizică (inclusive coduri de acces) trebuie să fie instalate în conformitate cu regulele Spitalului.

2. Accesul fizic la toate încăperile în care sunt instalate RICSOTGNT trebuie să fie documentat și monitorizat.

3. Toate încăperile la care sunt instalate RICSOTGNT trebuie să fie protejate fizic, în funcție de importanța acestora și tipul datelor vehiculate sau stocate.

4. Pentru fiecare încapere în care sunt instalate echipamente ale sistemului RICSOTGNT se aprobă accesul doar pentru personalul care răspunde de buna funcționare a echipamentelor din încaperea respectivă și, dacă este cazul, părților contractante, ale căror obligații contractuale implică acces.

5. Personalul care are drepturi de acces trebuie să detină legitimație de serviciu și/sau acte de identitate care să-i ateste calitatea.

6. Acordarea drepturilor de acces (folosind chei, parole etc.) se face în scris, de conducerea unității.

7. Nu este permis transferul dreptului de acces indiferent de motiv.

8. Cheile de acces care nu mai sunt folosite trebuie predate compartimentului care le-a eliberat.

9. Pierderea sau furtul cheilor de acces trebuie raportată imediat.

10. Cheile nu trebuie să aibă informații de identificare.

11. Accesul vizitatorilor în spațiile protejate trebuie documentat pentru fiecare încapere și, în cazul în care este permis, se va delega un însoțitor. Vizitatorii trebuie să fie însoțiti în zonele cu acces restrictionat.

10. Fiecare compartiment trebuie să verifice periodic drepturile de acces și să anuleze aceste drepturi pentru persoanele care pierd dreptul de acces.

Fiecare compartiment trebuie să anuleze drepturile de acces al cheilor utilizatorilor care își schimbă locul de muncă din Spital sau nu au relații contractuale cu Spitalul.

Anexa 3

Reguli de acces la rețeaua de comunicații a Spitalului

- 1.Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la rețea specificați Conducerea trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RICSOTGNT.
- 2.Conecțarea sistemelor de calcul care nu sunt proprietatea Spitalului se face numai cu aprobarea în scris a Managerului, la solicitarea șefilor de compartimente.
- 3.Accesul de la distanță la rețeaua Spitalului se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP) agrat de către Spital și folosind protocoale aprobate.
- Utilizatorii RICSOTGNT din interiorul Spitalului nu se pot conecta la altă rețea.
- 6.Utilizatorii nu trebuie să extindă sau să retransmită serviciile de rețea în niciun fel, pe nici o cale. Nu este permisă instalarea de conexiuni de rețea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face ia propunerea șefilor de compartimente.
- 7.Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de rețea, fără aprobarea conducerii.
- 8.Sistemele computerizate din afara Spitalului care necesită conectare la rețea trebuie a se conformeze cu standardele retelei interne a spitalului.
- 9.Utilizatorii nu au dreptul să descarce, să instaleze sau să ruleze programe de securitate care pot dezvăluia slabiciuni în securitatea unui sistem. Utilizatorii Spitalului nu au dreptul să ruleze programe de spargere a parolelor, sustragere de pachete, scanare a porturilor, în timp ce sunt conectați la rețeaua Spitalului.
10. Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de rețea, cabluri, prize de conexiuni.
11. Serviciul de nume și administrarea adreselor IP sunt deservite exclusiv de către administratorul de rețea.
12. Serviciile de interconectare a retelei Spitalului cu alte rețele sunt realizate exclusiv de către administratorul de rețea.
13. Nu este permisă instalarea și/sau modificarea echipamentelor utilizate pentru conectare la rețea (inclusiv placi de rețea) fără aprobarea administratorul de rețea.

Anexa 4

Reguli privind configurarea sistemelor informative pentru acces la rețeaua de comunicații

1. Infrastructura de comunicații, rețeaua de comunicații digitale a Spitalului este administrată de către administratorul de rețea.
2. Pentru a furniza o infrastructură de comunicații unitară cu posibilități de modernizare, toate componentele acesteia sunt instalate de către administratorul de rețea. Toate echipamentele, fără excepție, conectate la rețeaua de comunicații trebuie configurate conform specificațiilor administratorului de rețea.
- 3.Orice dispozitiv hardware, inclusiv plăcile de rețea, care se va conecta la rețeaua Spitalului, trebuie să fie însoțit de o aprobare de tip (producător, model, etc.) din partea administratorului de rețea.
- 4.Modificarea configurației oricărui dispozitiv activ conectat la rețeaua de comunicații se face numai de către administratorul de rețea.

5. Infrastructura de comunicatii de date a Spitalului suportă un set definit *de* protocole de rețea. Orice modificare a setului de protocole se face de către administratorul de rețea.
6. Adresele de rețea sunt alocate dinamic sau static numai de către administratorul de rețea.
7. Toate conectările în rețeaua de comunicatii a Spitalului sunt responsabilitatea administratorul de rețea
8. Toate conectările dintre rețeaua de comunicatii a Spitalului și alte retele de comunicatii, publice sau private, sunt responsabilitatea exclusiva a administratorului de rețea.
9. Echipamentele de protectie a retelei de comunicatie a Spitalului (*firewall*) se vor instala de către administratorul de rețea.
10. Utilizatorii nu au dreptul să extindă sau să retransmîtă în niciun fel serviciile retelei (este interzisa instalarea unui fax, modem, router, switch, hub sau punct de acces la rețeaua Spitalului) fără aprobare din partea conducerii.
11. Utilizatorilor li se interzice instalarea de dispozitive hardware rețea sau programe care furnizează servicii de rețea, fără aprobarea conducerii. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale retelei.

Anexa 5

Reguli de tratare a incidentelor de securitate

1. În cazul incidentelor de securitate din Spital, membrii conducerii Spitalului au functii și responsabilități predefinite, care pot fi prioritare îndatoririlor obișnuite.
2. Dacă un incident de securitate este suspectat sau confirmat (exemple: virus, vierme, descoperirea unor activități suspecte, informații modificate, etc.), trebuie urmate procedurile standard specifice pentru micșorarea riscurilor.
3. Administratorul rețelei este responsabil cu înștiintarea și coordonarea pentru tratarea incidentului, strangerea dovezilor fizice și electronice ce vor face parte din documentația pentru tratarea incidentului.
5. Folosind resurse tehnice speciale se va monitoriza nivelui daunelor și gradului de eliminare sau atenuare a vulnerabilităților, acolo unde este cazul.
6. Administratorul rețelei, împreună cu managerul, stabilesc continutul comunicatelor pentru utilizatori privind incidentele și vor determina nivelul și modul de distribuire a acestor informații.
7. Administratorul rețelei trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informațiile utile pentru eliminarea sau diminuarea vulnerabilităților care au cauzat incidentul.
8. Administratorul rețelei este responsabil cu documentarea anchetei privind incidentul. Administratorul rețelei este responsabil de coordonarea activităților de comunicare cu terții, pentru rezolvarea incidentului.
10. În cazul în care incidentul nu implică actiuni contrare legilor în vigoare, administratorul rețelei va recomanda sanctiuni disciplinare.
11. În cazul în care incidentul implică aplicarea legilor civile sau penale, administratorul rețelei va recomanda managerului sesizarea organelor în drept ale statului și va actiona ca persoană de legătură cu acestea.

Anexa 6

Reguli de monitorizare a Resurselor informatice și de Comunicații

Monitorizarea RICSOTGNT se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatici și a situațiilor de încălcare a regulamentelor de securitate.

Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări și înregistra:

- Tipul traficului (ex. structura pe protocole și servicii) extern și continutul acestuia în cazurile în care acest lucru se impune sau este ordonat;
- Tipul protocoalelor și a echipamentelor conectate la RICSOTGNT, continutul acestuia în cazurile în care acest lucru se impune sau este ordonat
- Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).
- Fișierele jurnal vor fi examineate regulat în vederea detectării eventualelor atacuri informatiche și abateri de la regulamentele de securitate ale Spitalului.

În această categorie intră următoarele (fără a se limita doar la acestea):

- Jurnale ale sistemelor de detectare automată a intrușilor,
- Jurnale Firewall;
- Jurnale ale activității conturilor utilizator;
- Jurnale ale scanărilor relea;
- Jurnale ale aplicațiilor;
- Jurnale ale solicitărilor de suport tehnic;
- Jurnale ale erorilor din sisteme și servere.

Administratorul rețelei va efectua, în mod regulat (cel puțin o dată la șase luni), verificări pentru detectarea:

- Echipamentelor de rețea conectate neautorizat;
- Serviciilor de rețea neautorizate;
- Serverelor de pagini de web neautorizate;
- Echipamentelor ce utilizează resurse comune nesecurizate;
- Licentelor pentru sistemele de operare și programelor instalate.

Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către conducere în scopul efectuării de investigații.

Anexa 7

Reguli pentru detectarea accesului neautorizat

1. Procesele de înregistrare și verificare a activității sistemelor de operare, conturilor utilizator, programelor trebuie să fie funcționale pe toate sistemele active (host, server, echipamente de rețea).
2. Trebuie activate funcțiile de anunțare a persoanelor responsabile oferite de *firewall-uri* și sistemele de control al accesului la rețea.
3. Trebuie activate funcțiile de înregistrare a evenimentelor pe dispozitivele firewall și pe toate sistemele de control al accesului.
4. Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate și revizuite (examineate) zilnic de către administratorul de sistem sau trebuie instituit un sistem automatizat de avertizare.
5. Verificările privind integritatea fiecărui trebuie să se facă periodic. Aceasta activitate este obligatorie și pentru dispozitivele de tip *firewall* sau dispozitive de control al accesului.
6. Înregistrările de verificare pentru serverele și host-urile din rețeaua internă trebuie revizuite cel puțin săptămânal sau trebuie instituit un sistem automatizat de avertizare.
7. Se vor verifica periodic programele utilizare pentru detectarea tentativelor de acces neautorizat.
8. Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de sistem a unor activități ce ar putea implica o activitate de acces neautorizat.
9. Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către conducerea unitatii .

10. Utilizatorii sunt obligati să raporteze conducerii și administratorului de sistem orice anomalii privind performanța sistemelor utilizate sau orice elemente ale unor posibile infracțiuni.

Anexa 8

Reguli privind crearea și utilizarea copiilor de siguranță (*backup*)

1. Frecvența, dimensiunea și continutul copiilor de siguranță trebuie să fie în concordanță cu importanța informației și *cu* riscul acceptat de proprietarul datelor.
2. Procedura de creare a copiilor de siguranță și de recuperare pentru fiecare sistem din cadrul RICSOTGNT trebuie să fie documentată și periodic revizuită.
3. Procedurile stabilite între Spital și furnizorii de stocare a copiilor de siguranță în altă zonă trebuie să fie revizuite cel puțin anual.
4. Copiile de siguranță trebuie să fie periodic testate pentru a asigura faptul că informațiile stocate sunt recuperabile.
5. Accesul la mediile de backup ale Spitalului, stocate la furnizori extern sau în interior se va face folosindu-se procedurile specifice de acces. Acestea trebuie revizuite periodic (anual). Accesul trebuie interzis pentru persoanele autorizate care își schimbă locul de muncă.
6. Mediile utilizate pentru stocarea copiilor de siguranță trebuie să aibă un sistem de identificare care să conțină cel puțin următoarele date de identificare a informației stocate:
 - numele sistemului;
 - data creării copiei;
 - tipul de copie (completă, incremental, etc.);
 - clasificarea sensibilității (sigurantei/securității);

Anexa 9

Reguli privind securitatea informațiilor în cazul utilizării calculatoarelor/dispozitivelor portabile

1. Calculatoarele portabile trebuie să fie protejate prin parole.
2. Se va evita stocarea datelor care privesc Spitalul pe dispozitivele portabile.
3. În cazul în care nu există altă alternativă de stocare locală toate datele care privesc Spitalul trebuie criptate utilizând tehnici aprobate.
4. Transmiterea datelor prin retele de tip wireless se poate face numai prin retelele instalate de către administratorul de rețea; acestea vor utiliza tehnici de criptare pentru protejarea datelor transmise.
5. Toate accesările de la distanță a Resurselor Informatici și de Comunicații trebuie să se efectueze prin intermediul serviciului autorizat, conform *Regulilor de acces la rețeaua de comunicații*.
6. Conectarea sistemelor de calcul care nu sunt proprietatea Spitalului se face numai cu aprobarea scrisă a managerului unității

Anexa 10

Reguli de administrare a conturilor de email

1. Fiecare cont de email creat trebuie să aibă asociate o cerere și o aprobare corespunzătoare.
2. Tutti utilizatorii sunt obligati să păstreze confidențialitatea informațiilor privind contul de acces.
3. Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.

4. La cererea conducerii, administratorul de rețea trebuie să furnizeze lista cu toți utilizatorii (lista de conturi) pentru sistemele pe care le administrează.

Anexa 11

Reguli privind sistemul de mesagerie electronică

1. Activități strict interzise

Trimiterea de mesaje cu caracter de intimidare sau hărțuire;

Folosirea sistemului de mesagerie electronică în scopuri personale;

Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;

Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;

Folosirea altor identități decât cea reală atunci când se trimit emailuri, exceptând cazurile cind persoana este autorizată în scop de suport administrativ.

2. Activități interzise deoarece împiedică buna funcționare a comunicatiilor în rețea și eficiența sistemelor de mesagerie electronică:

- Trimiterea mesajelor nesolicitante către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituția;

Trimiterea sau retrimiterea mesajelor care pot conține viruși;

Ignorarea cererii administratorului rețelei de a elibera spațiile de pe server pe care le ocupă.

Toate informațiile și datele confidențiale ale Spitalului, transmise către alte rețele externe, trebuie să fie criptate.

Anexa 12

Reguli de detectare a virușilor

1. Toate stațiile de lucru de sine stătătoare sau conectate la rețeaua de comunicații a Spitalului trebuie să utilizeze programe antivirus aprobată de către administratorul de sistem.

2. Programele antivirus nu trebuie să poată fi dezactivate de către utilizatori. Acestea trebuie să fie tot timpul active.

3. Configurația programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.

4. Frecvența actualizărilor automate a programului antivirus trebuie să fie zilnică. Orice server de fișiere conectat la rețeaua instituției trebuie să utilizeze un program antivirus aprobat.

5. Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat și trebuie să respecte regulile de instalare și de utilizare a acestui program.

6. Orice virus care nu a putut fi înălțat automat de către programul antivirus constituie un incident de securitate și trebuie să fie raportat imediat administratorului de sistem în mod automat.

Anexa 13

Reguli de relații cu terții

1. În toate convențiile și contractele încheiate cu furnizorii trebuie specificate:

-informațiile din cadrul Spitalului la care Furnizorul are drept de acces;

-modul în care informațiile la care Furnizorul are drept de acces urmează să fie protejate de aceasta, precum și măsuri ce vor fi luate în cazul nerespectării clauzelor;

-metodele *dă* predare, distrugere sau de transfer at drepturilor informatiilor Spitalului aflate în posesia Furnizorului la încheierea contractului.

2. Furnizorul trebuie să folosească sistemul RICSOTGNT din cadrul Spitalului numai în scopul stipulat în contract.

3. Once alta informatie din sistemul RICSOTGNT obținuta de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.

4. Toate echipamentele de întreținere ale Furnizorului aflate în rețeaua internă a Spitalului și care se pot conecta în exterior prin intermediul rețetei, precum și toate conturile de utilizator create temporar pentru Furnizor și necesare pentru acces la RICSOTGNT vor fi scoase din uz la încheierea relațiilor contractuale.

5. Activitatile principale ale Furnizorului trebuie să fie documentate de acesta și puse la dispozitia conducerii Spitalului, la cerere. Acestea trebuie să cuprinda, dar să nu fie limitate la evenimente precum: schimbări de personal, schimbări de parole, schimbări majore în derularea proiectului, timpii de sosire, de plecare și de livrare.

6. În cazul retragерii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informatiile sensibile sunt colectate și predate Spitalului sau distruse în cel mult 24 de ore de la producerea evenimentului.

7. În cazul terminării sau rezilierii contractului la cererea Spitalului, Furnizorul va preda sau distrugе toate informatiile ce aparțin Spitalului și va oferi certificare în acest sens privind predarea sau distrugerea informatiilor în decurs de 24 de ore de la producerea evenimentului.

8. În cazul încheierii contractului sau la cererea Spitalului, Furnizorul trebuie să predea imediat toate legitimiatiile, echipamentele și stocurile Spitalului. Echipamentele și/sau stocurile care urmează a fi reținute de către Furnizor trebuesc documentate și autorizate de conducerea Spitalului.

9. Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către Spital trebuie să fie inventariate corespunzător și să posede drepturi de utilizare atestate prin licente.