APROBAT
MANAGER
Dr. Sanda PATRICHI

Politica de securitate a Sistemului Informational

şi Regulamentul de Securitate
privind
RESURSELE INFORMATICE ŞI DE COMUNICAŢII

din cadrul
SPITALULUI CLINIC DE RECUPERARE CLUJ - NAPOCA

Cuprins

Cap. I Politica de Securitate privind Sistemul Informational

1.1 Introducere

Sistemului informaţional este o componentă a managementului organizaţiei care încorporeaza totalitatea resurselor informaţionale create, prelucrate şi transmise pe fluxuri şi circuite informaţionale , precum şi a tehnicilor şi mijloacelor de procesare a acestora în vederea creşterii rapidităţii şi fiabilităţii actului decizional. Ca urmare apare la nivelul organizaţiei nevoia dezvoltării unui sistem eficient de procurare, prelucrare şi stocare a acestor informaţii care să fie în masură să le transforme în resurse disponibile şi refolosibile subsumate fundamentării corespunzătoare a deciziilor privind activitatea curentă şi de perspectivă a organizaţiei.

Compromiterea securităţii Sistemului Informational poate afecta capacitatea SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA de a oferi serviciile specifice, poate conduce la fraude sau distrugerea datelor, violarea clauzelor contractuale, divulgarea secretelor, afectarea credibilităţii SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA în faţa pacientilor si partenerilor săi.

Această politică este stabilită astfel încât:

- Să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informationale publice si private;
- Să stabilească practici prudente şi acceptabile privind utilizarea Resurselor Informationale si de Comunicatii (denumite in continuare RIC) ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA ;
- Să instruiască utilizatorii care au dreptul de folosire a sistemului RIC privind responsabilităţile asociate unei astfel de utilizări.

Politica de securitate a Sistemului Informationa; al SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informational şi de comunicaţii (incluzand ambele forme de prezentare a informatiei : digitala sau letrica) a SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .

Următoarele entităţi şi utilizatori sunt vizaţi în mod distinct de prevederile Politicii:

- Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- Colaboratorii SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA care au acces la sistemul RIC;
- Furnizorii SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA care au acces la sistemul RIC;
- Voluntarii care desfasoara activitati in SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA ;
- Alte persoane, entităţi sau organizaţii care au acces la sistemul RIC.

1.2 Scopul politicii de securitate

Politica de securitate a Sistemului Informational are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei.

Confidenţialitatea se referă la asigurarea faptului ca informatia este accesibila doar persoanelor autorizate .

Integritatea se referă la măsurile şi procedurile utilizate pentru asigurarea acuitatii , complitudinii si protecţiei datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor Sistemului Informational..

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor şi procedurilor de securitate. Acestea sunt obligatorii pentru toţi utilizatorii Sistemului Informational.

1.3 Definiţii folosite în politica de securitate şi regulamentul de utilizare

Sistem Informational : ansamblul de elemente format din :

- ***resursele informationale*** = informatiile generate, obtinute, disponibile şi refoloşibile; fiecare activitate la randul ei genereaza noi informatii care la randul lor sunt utile ducerii la bun sfarşit a acelei activitati sau a altora
- ***circuitele şi fluxurile informationale*** = maximul de informaţie utilă trebuie sa fie transferata de la emitator la beneficiar pe calea cea mai scurtă
- ***procedurile informationale*** = metodele şi tehnicile de culegere, inregistrare şi prelucrare, operaţiile componente, suportii, formulele, modelele de tratare a informaţiilor
- ***mijloacele de tratare a informatiilor (suportul tehnic)*** = ansamblu unitar al mijloacelor de culegere al datelor, inregistrare , transmitere şi prelucrare a informatiilor

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 (notebook-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), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, 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 creea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.

În acord cu prevederile din prezentul document, **R**esursele **I**nformationale şi de **C**omunicaţii (RIC) sunt bunuri strategice ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA care trebuiesc administrate ca resurse proprii ale organizatiei

Administratorul Resurselor Informatice şi de Comunicaţii (ARIC): Responsabil la nivelul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA cu administrarea şi finanţarea RIC. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Titlul este atribuit în mod automat ordonatorului de credite, adică managerului.

Ofiţer responsabil cu Securitatea RIC (OSRIC): Răspunde direct doar în faţa ARIC privind administrarea funcţiilor de securitate a informaţiei în cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA . Este persoana de contact intern şi extern a SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA pentru orice problemă în legătură cu securitatea RIC. Funcţia OSRIC este atribuită responsabilului sistemului informational .

Ofiţer responsabil cu securitatea RIC la nivel Departamental (OSRICD): Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament. Funcţia *OSRICD* este atribuită şefului de serviciu, birou, departament.

Utilizator: O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC.

Abuz de privilegii: Orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA 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 şi/sau servicii SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA în baza unui contract comercial sau de colaborare.
Internet: Sistem global care interconectează calculatoare şi reţele de calculatoare. Acestea sunt deţinute de mai multe organizaţii, agenţii guvernamentale, societăţi, instituţii academice.

Intranet: Reţea privată destinată comunicaţiilor şi partajării informaţiilor, care, ca şi reţeaua Internet, foloseşte suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizaţi din cadrul unei organizaţii (instituţii). În mod obişnuit, reţeaua Intranet a unei organizaţii este protejată printr-un sistem de protecţie (firewall).

Structura de Securitate a Sistemului Informational (SSSI) / Echipa de Răspuns la Incidentele de Securitate a RIC (ERIS): persoanele responsabile de acţiunile desfăşurate în scopul micşorării sau eliminării impactului negativ al unui incident de securitate. ERIS este formata din ARIC, OSRIC, OSRICD.
Fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , sunt proprietatea instituţiei în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la sistemul RIC
Virus: Un program care se auto-ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte de la cele deranjante până la cele distructive. Un virus se execută în momentul în care este accesat un fişier infectat. Un virus de macro infectează codul executabil încapsulat în pachetul de programe Microsoft Office (Word, Excel, PowerPoint) sau alte programe care permit utilizatorului să genereze macro-uri.

Vierme: Un program care se auto-copiază în oricare altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul reţelei. Prima utilizare a termenului descria un program care s-a multiplicat într-o reţea de calculatoare, folosind resursele sau calculatoarele neutilizate din reţea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o ameninţare la adresa securităţii datorită faptului că folosesc reţeaua pentru a se împrăştia, împotriva voinţei proprietarilor de sisteme de calcul, cauzând astfel nefuncţionarea sau funcţionarea defectuoasă a reţelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferenţa constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere pentru a se multiplica.

Cal troian: de obicei un virus sau un vierme – care este ascuns sub forma unui program atractiv sau inofensiv, cum ar fi un joc, sau program de grafică (o felicitare în format electronic, un program tip screen-saver). Victimele pot primi un astfel de cal troian prin email sau pe o dischetă, adeseori de la o altă victimă necunoscută sau pot fi încurajate să descarce un fişier de pe o pagină Web sau un forum.

Incident de Securitate: În termeni informatici este definit ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrităţii şi/sau confidenţialităţii informaţiei de pe un sistem informatic automatizat. Aceasta include examinarea sau navigarea neautorizată, întreruperea sau anularea unui serviciu, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea informaţiilor, modificarea informaţiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştiinţa sau intenţia utilizatorului.

Reţea locală (LAN): O reţea de comunicaţii de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Reţeaua locală oferă comunicaţii între calculatoare şi periferice la o viteză de transfer mare şi cu puţine erori.

Server: Un program de calculator care oferă servicii altor programe aflate pe acelaşi calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe acelaşi calculator mai pot rula şi alte programe de tip client sau server.

Gazdă (Host): Un sistem care oferă servicii pentru un anumit număr de utilizatori.

Copii de Siguranţă (backup): Copii ale fişierelor şi aplicaţiilor făcute pentru a evita pierderea datelor şi pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.

Firewall: Un mecanism de control al accesului care acţionează ca o barieră între două sau mai multe segmente ale unei reţele de calculatoare sau ale unei arhitecturi de tip client/server, folosit pentru a proteja reţelele interne sau segmente ale acestora împotriva utilizatorilor sau proceselor neautorizate.

Atac informaţional: O încercare de a trece peste măsurile şi controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului de RIC. Atacatorul poate altera informaţiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular şi de eficacitatea contramăsurilor aplicate.

Protecţie informaţională: Acţiuni întreprinse în vederea afectării informaţiilor şi sistemelor informatice ostile, în timp ce protejează informaţiile şi sistemele informatice proprii.

Procedura / instructiune de lucru - reprezintă modalitatea specifică de desfăşurare a unei activităţi sau a unui proces.

1.4 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
- Strict Secrete

ARIC, OSRIC, OSRICD, conducerea instituţiei răspund de evaluarea periodică a schemei de clasificare a informaţiilor. Toate informaţiile din Spitalului Clinic de Recuperare Cluj-Napoca trebuie să se regăsească în una din următoarele categorii:

1. ***Publice.*** Acestea sunt informaţiile accesibile oricărui utilizator din interiorul sau exteriorul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA . Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA sau aceste efecte sunt nesemnificative. Utilizatorii care furnizează aceste informaţii sunt responsabili de asigurarea integrităţii şi disponibilităţii acestora în raport cu cerinţele SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
2. ***Secrete.*** În această categorie se includ informaţiile pe care SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA trebuie să le protejeze conform legislaţiei în vigoare. Aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate şi distribuite în cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA doar utilizatorilor autorizaţi. Distribuirea acestor informaţii de către utilizatorii autorizaţi trebuie să se facă pe baza unei clauze de confidenţialitate.
3. ***Strict Secrete sau Confidenţiale.*** În această categorie se includ toate informaţiile care datorită valorii naturii lor nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidenţa Codului Civil, Penal sau legislaţiei în vigoare. Accesul la aceste informaţii va fi restricţionat. Datele strict secrete nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .

1.5 Confidenţialitate

1. Fişierele electronice create, trimise, primite sau stocate folosind sistemul RIC propriu, administrate sau în custodia şi sub controlul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA nu au caracter personal şi pot fi accesate oricând de către angajaţii autorizaţi (specialistul IT/administrator reţea) fără înştiinţarea utilizatorului.
2. În scopul administrării RIC şi pentru asigurarea securităţii RIC personalul autorizat poate revizui sau utiliza orice informaţie stocată pe sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor.
3. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea OSRIC sau OSRICD).
4. Un mare număr de utilizatori, pot accesa diverse informaţii din sistemul de comunicaţii al SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA. În aceste condiţii este obligatorie păstrarea confidenţialităţii acestor informaţiilor transmise din exteriorul RIC şi a informaţiilor obţinute din interior.

5. Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA pentru care nu au autorizaţie sau consimţământ explicit.
6. Nici un utilizator al sistemului RIC ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului RIC. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , conform angajamentelor personale sau contractelor de munca semnate, existente in cadrul Departamentului Resurse Umane.
7. 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 SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

Cap. II Regulamentele de Utilizare a Resurselor Informatice şi de Comunicaţii (RIC)

Introducere

Regulamentele de Utilizare a Resurselor Informatice şi de Comunicaţii sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA . Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea acestea au ca scop protejarea imaginii instituţiei şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţii.

În acord cu legislaţia în vigoare în România, Regulamentele de ordine interioară ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , Resursele Informatice şi de Comunicaţii sunt valori ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA care trebuie exploatate şi administrate ca resurse publice în proprietatea SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA.

Scopul acestor regulamente este acela de a asigura:

- Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea RIC în vederea sprijinirii activitatii medicale si administrativ;
- Protejarea imaginii SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA ;
- Protejarea investiţiilor SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA pentru dezvoltarea RIC proprii;
- Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate folosind RIC ale utilizatorilor autorizaţi: membrii conducerii , personal contractual, voluntari, colaboratori etc.
- Educarea utilizatorilor RIC în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;

- Compatibilitate cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea RIC .

Regulamentele de utilizare a RIC ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acesta.

Prevederile Politicii de Securitate şi Procedurile de Lucru aprobate vor fi aplicate tuturor entităţilor şi utilizatorilor după cum urmează:

- Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- Colaboratorii SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA care au acces la sistemul RIC;
- Furnizorii SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA care au acces la sistemul RIC;
- Voluntarii care desfasoara activitati in SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA ;
- Alte persoane, entităţi sau organizaţii care au acces la sistemul RIC.

Modificarea regulamentului şi/sau a procedurilor / instructiunilor generale de lucru se va face ori de câte ori este nevoie, iar aprobarea modificărilor se va face de către conducere la propunerea OSRIC.

Instructiunile Generale de Lucru fac parte integrantă din prezentul regulament şi sunt prezentate în anexa 1.

2.1 Regulament de utilizare a RIC

1. Utilizarea sistemului RIC se face numai în interes de serviciu.
2. Utilizatorii trebuie să anunţe OSRIC sau OSRICD în cazul în care se observă orice problemă/breşă în sistemul de securitate a RIC din cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.
3. Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip în cadrul sistemului RIC al SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
4. Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din RIC pentru care nu au autorizaţie sau consimţământ explicit.
5. Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive şi/sau informaţii similare utilizate în scopuri de autorizare şi identificare.
6. Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).
7. Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea OSRIC, cu excepţia cazului în care acestea se găsesc pe lista programelor standard folosite în cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA . Această listă va fi întocmită de către OSRIC împreună cu OSRICD în funcţie de necesităţile departamentelor.
8. Utilizatorii nu trebuie:
   - să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane;
   - să degradeze performanţele RIC;
   - să împiedice accesul unui utilizator autorizat la RIC;
   - să obţină alte resurse în afara celor alocate;

- să nu ia în considerare măsurile de securitate impuse prin regulamente;
- să exploateze defectuos componentele RIC;
- să utilizeze dischete, cd-uri, sau orice alt suport magnetic de stocare a informaţiei din exteriorul instituţiei fără acordul explicit al OSIRC.

9. Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii RIC. De exemplu, utilizatorii din SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente.
10. RIC ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA nu trebuiesc folosite pentru beneficiul personal.
11. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA le poate considera ofensive, indecente sau obscene (altele decât cele pentru care aprobarea explicită a conducerii instituţiei).
12. Accesul la reţeaua Internet prin intermediul RIC se supune aceloraşi regulamente care se aplică utilizării din interiorul instituţiei şi **Regulamentului pentru Utilizare Internet şi Intranet (cap.II subcap.14)**.
13. Angajaţii nu trebuie să permită membrilor familiei sau altor persoane străine neautorizate, care nu au aprobare explicită din partea ARIC, OSRIC, sau a conducerii instituţiei accesul la RIC ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
14. Utilizatorii care au acces la RIC al Spitalul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA au obligaţia de a purta acte şi/sau legitimaţii/ecusoane care să ateste calitatea de utilizator autorizat în spaţiile SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
15. Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA folosind RIC.
16. În cazul demisiei/plecării definitive din instituţie a unui utilizator acest lucru va fi comunicat OSRIC de către OSRICD şi/sau Serviciul Resurse Umane din Cadrul instituţiei. OSRIC va recurge la stergerea conturilor şi parolelor utilizatorului respectiv, iar accesul utilizatorului la RIC va fi interzis.
17. Este interzisă utilizarea RIC de către persoane neautorizate.

2.2. Utilizarea ocazională a RIC în scopuri personale

În aceste situaţii se aplică următoarele restricţii:

1. Utilizarea personală ocazională a serviciilor de poştă electronică, acces internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricţionată la utilizatorii autorizaţi şi nu poate fi extinsă la membrii familiilor sau alte persoane.
2. Utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
3. Utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaţilor.
4. Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA sau prejudicierea, indiferent de formă, a intereselor Instituţiei.
5. Stocarea mesajelor de email, a mesajelor de voce, a documentelor şi fişierelor personale din cadrul RIC trebuie să fie nominală.
6. Toate mesajele, fişierele şi documentele – incluzând mesajele personale, fişierele şi documentele – localizate în cadrul RIC sunt proprietatea Instituţiei şi pot fi subiectul unor

cereri de verificare/inspectare/accesare de către ARIC, OSRIC sau OSRICD conform regulamentelor.

2.3. Accesul Administrativ

1. Utilizatorii trebuie să cunoască şi să accepte toate regulamentele privind securitatea RIC înainte de a li se permite accesul la un cont.
2. Utilizatorii care au conturi de acces administrativ trebuie sa aibă instrucţiuni de administrare, documentare, instruire şi autorizare a conturilor. Aceste instrucţiuni se vor elabora de către fiecare Departament şi vor fi incluse în fişa postului.
3. Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi şi trebuie să facă investigaţii numai sub îndrumarea OSRIC sau OSRICD.
4. Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activităţii pe care o desfăşoară.
5. Accesul administrativ trebuie să se conformeze **Regulamentului privind Parolelor (cap.II subcap.2.16)** .
6. Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al OSRIC şi trebuie să fie schimbată atunci când o persoana care utilizează acest cont îşi schimbă locul de muncă din cadrul Departamentului sau a Instituţiei, sau în cazul unei modificări a listei de personal ale terţilor (furnizor desemnat) în contractele cu SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
7. Trebuie să existe o procedură prin care o altă persoană, în afară de administrator, să poată avea acces la contul administratorului în caz de forţa majoră. Această procedură va fi elaborată de către OSRIC şi comunicată OSRICD aflat în cauză.
8. Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operaţiuni definite. Acestea trebuie să îndeplinească următoarele condiţii:
   - trebuie să fie autorizate;
   - trebuiesc create cu dată de expirare specifică;
   - contul va fi şters atunci când nu mai este necesar.

2.4. Accesul Fizic

1. Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat şi monitorizat.
2. Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.
3. Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RIC se aprobă accesul doar pentru personalul care răspunde de buna funcţionare a echipamentelor din încăperea respectivă şi, dacă este cazul, părţilor contractante, ale căror obligaţii contractuale implică acces fizic.
4. Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.
5. Nu este permis transferul dreptului de acces indiferent de motiv.
6. Accesul publicului, vizitatorilor, sau a persoanelor străine în cadrul instituţiei se va face doar pe baza actului de identitate. Vizitatorii/persoanele străine trebuie să fie însoţiţi în zonele cu acces restricţionat.
7. Pentru fiecare spaţiu în care sunt instalate RIC se va păstra o evidenţă a accesului pentru verificări de rutină în situaţii critice.

2.5. Conectarea la Sistemul Resurselor Informatice şi de Comunicaţii

1. Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către administratorul de reţea .
2. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele şi datele de identificare ale acesteia se vor comunica către OSRIC.
3. Conectarea sistemelor de calcul care nu sunt proprietatea SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA se face numai cu aprobarea în scris din partea conducerii instituţiei.
4. Accesul de la distanţă la reţeaua SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA şi folosind protocoale aprobate de către OSRIC.
5. Utilizatorii RIC din interiorul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA nu se pot conecta la altă reţea.
6. Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel (pe nici o cale). Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Departamentelor de către ARIC la propunerea OSRIC.
7. Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea ARIC la propunerea OSRIC.
8. Sistemele computerizate din afara Instituţiei care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
9. Utilizatorii nu au dreptul să descarce din Internet, să instaleze sau să ruleze programe de securitate sau de altă natură care pot dezvălui slăbiciuni în securitatea unui sistem. De exemplu, utilizatorii SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua Instituţiei.
10. Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.
11. Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către OSRIC.
12. Serviciile de interconectare a reţelei SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA cu alte reţele sunt realizate exclusiv de către OSRIC.
13. Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea ARIC la propunerea OSRIC. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către OSRIC.

2.6. Configurarea Parametrilor de Acces la Reţea

1. Infrastructura de comunicaţii, reţeaua de comunicaţii digitale, a SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA este administrată de către OSRIC care este responsabil cu întreţinerea şi dezvoltarea acesteia.
2. Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare toate componentele acesteia sunt instalate de către OSRIC sau de către un furnizor avizat explicit de către OSRIC .

3. Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor OSRIC .
4. Orice dispozitiv hardware, inclusiv plăcile de reţea şi modemuri, care se va conecta la reţeaua SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , trebuie să fie însoţit de o aprobare de tip (producător, model etc.) din partea ARIC la propunerea OSRIC.
5. Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai de către OSRIC.
6. Infrastructura de comunicaţii de date a SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA suportă un set definit de protocoale de reţea (TCP/IP). Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către ARIC .
7. Adresele de reţea sunt alocate dinamic sau static numai de către OSRIC.
8. Toate conectările în reţeaua de comunicaţii a SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA sunt responsabilitatea OSRIC, conectarea se va face numai în baza unei cereri standard aprobată de către conducerea Instituţiei.
9. Toate conectările dintre reţeaua de comunicaţii a SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a OSRIC .
10. Echipamentele de protecţie a reţelei de comunicaţie a SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA (firewall) se vor instala de către OSRIC sau de către un furnizor avizat explicit de către OSRIC.
11. Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei (este interzisă instalarea unui telefon, fax, modem, router, switch, hub sau punct de acces la reţeaua Instituţiei fără aprobare din partea ARIC. Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau programe care furnizează servicii de reţea fără aprobarea ARIC la propunerea OSRIC.
12. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

2.7. Tratarea Incidentelor de Securitate şi de nerespectare a Politicii şi Regulamentului de Securitate

Membrii Echipei de Răspuns la Incidentele de Securitate (Membrii ERIS) ai ric , au funcţii şi responsabilităţi pre-definite care pot fi prioritare îndatoririlor obişnuite. Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc., trebuie urmate procedurile standard specifice pentru micşorarea riscurilor.

OSRIC este responsabil cu înştiinţarea şi coordonarea echipei ERIS pentru tratarea incidentului.

OSRIC este responsabil cu strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului. Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităţilor acolo unde este cazul.

OSRIC, în colaborare cu ARIC va stabili conţinutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informaţii.

OSRIC şi ERIS trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.

OSRIC este responsabil cu documentarea anchetei privind incidentul cu asistenţă din partea ERIS.

OSRIC este responsabil de coordonarea activităţilor de comunicare cu terţi pentru rezolvarea incidentului.

În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare OSRIC va recomanda ARIC sancţiuni disciplinare.

În cazul în care incidentul implică aplicarea legilor civile sau penale OSRIC va recomanda ARIC sesizarea organelor în drept ale statului şi va acţiona ca ofiţer de legătură cu acestea.

2.8. Monitorizarea Resurselor Informatice şi de Comunicaţii

Monitorizarea RIC se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice şi a situaţiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări şi înregistra:

- Tipul traficului (ex. structura pe protocoale şi servicii) extern şi conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
- Tipul traficului în reţea, a protocoalelor şi a echipamentelor conectate la RIC, conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
- Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .

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

- Jurnale ale sistemelor de detectarea automată a intruşilor.
- Jurnale Firewall
- Jurnale ale activităţii conturilor utilizator
- Jurnale ale scanărilor reţea
- Jurnale ale aplicaţiilor
- Jurnale ale erorilor din sisteme şi servere.

2.9. Securitatea Serverelor

Un server nu trebuie conectat la reţeaua SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA până când nu se află într-o stare sigură acreditată de către OSRIC.

Procedura de securizare a serverelor trebuie să includă obligatoriu următoarele:

- Instalarea sistemului de operare dintr-o sursă aprobată
- aplicarea patch-urilor furnizate de producător
- înlăturarea programelor, a serviciilor sistem şi a driver-lor care nu sunt necesare
- setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare
- dezactivarea sau schimbarea parolelor conturilor predefinite
- securizarea accesului fizic la aceste echipamente

OSRIC va monitoriza obligatoriu pentru serverele principale (enterprise) procesul de instalare şi aplicare regulată a patch-urilor de securitate şi, prin sondaj, pentru serverele departamentale sau a grupurilor de lucru.

2.10 Crearea şi Utilizarea Copiilor de Siguranţă (Backup)

1. Frecvenţa, dimensiunea şi conţinutul copiilor de siguranţă trebuie să fie în concordanţă cu importanţa informaţiei şi cu riscul acceptat de proprietarul datelor.
2. Procedura de creare a copiilor de siguranţă şi de recuperare pentru fiecare sistem din cadrul RIC trebuie să fie documentată şi periodic revizuită.
3. Verificarea copiilor de siguranţă se va face după o procedură documentată şi revizuită periodic.
4. Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţiile stocate sunt recuperabile.
5. Accesul la mediile de backup ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA se va face numai de personalul abilitat în acest sens.
6. Accesul trebuie interzis pentru persoanele autorizate care îşi schimbă locul de muncă.

2.11 Detectarea Tentativelor de Acces Neautorizat

1. Procesele de înregistrare şi verificare a activităţii sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcţionale pe toate sistemele active (host, server, echipamente de reţea).
2. Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la reţea.
3. Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.
4. Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către administratorul de sistem.
5. Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip firewall sau dispozitive de control al accesului.
6. Înregistrările de verificare pentru serverele şi host-urile din reţeaua internă trebuie revizuite cel puţin săptămânal.
7. Se vor verifica periodic (săptămânal) programele utilitare pentru detectarea tentativelor de acces neautorizat.
8. Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii 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 OSRIC.
10. Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile infracţiuni la OSRIC sau OSRICD.

2.12 Utilizarea Calculatoarelor Portabile

1. OSRIC trebuie să aprobe, în scris, conectarea dispozitivelor portabile la RIC ale organizatiei.
2. Calculatoarele portabile trebuie să fie protejate prin parole.
3. Se va evita stocarea datelor care privesc SC MEDICAL CENTER SRL pe dispozitivele portabile. În cazul în care nu există o altă alternativă de stocare locală, toate datele care privesc SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA trebuiesc criptate.
4. Conectarea sistemelor de calcul care nu sunt proprietatea SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA se face numai cu aprobarea în scris a ARIC la recomandarea OSRIC.

5. Dispozitivele portabile de calcul neutilizate trebuie securizate fizic. Aceasta presupune încuierea lor într-un birou, într-un dulap.

2.13 Modificări şi Modernizări ale Sistemului Resurselor Informatice şi de Comunicaţii

1. Orice modificare asupra unei componente a RIC din cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă prezentului regulament şi trebuie să urmeze procedurile în vigoare.
2. OSRIC trebuie să fie anunţat de toate modificările care afectează mediul de funcţionare a sistemelor componente ale RIC (ex: aparate de aer condiţionat, instalaţii de apă, încălzire, instalaţii electrice şi alarme, etc.).
3. Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RIC vor fi documentate şi aprobate de către ARIC. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RIC.
4. Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducerea instituţiei.

2.14 Utilizare Internet şi Intranet

1. Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopuri exclusiv de servici, cu excepţia situaţiei prevăzute în regulamentul **Utilizarea ocazională a RIC în scopuri personale (cap.II subcap.2.2)**.
2. Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către ASRIC la propunerea OSRIC. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie de către producător.
3. Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore.
4. Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy şi/sau firewall.
5. Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze **Regulamentului de Utilizare Acceptabilă a RIC(cap.II subcap.2.1)**.
6. Orice activitate a utilizatorilor folosind RIC poate fi înregistrată şi ulterior examinată.
7. Nu se vor publica pe sit-urile web ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA materiale cu caracter ofensiv sau de hărţuire.
8. Nu se vor publica pe sit-urile web ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , materiale publicitare comerciale sau personale.
9. Nu se vor publica pe site-urile web ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA date ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA fără asigurarea că materialele sunt disponibile numai persoanelor sau grupurilor autorizate.
10. Nu este permisă utilizarea RIC ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA în scop personal sau pentru solicitări personale ce nu au legătură cu SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
11. Cumpărăturile pe internet care nu au legătură cu atribuţiile de serviciu sunt interzise. Cumpărăturile în interes de serviciu se vor supune regulilor de achiziţie ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .

12. Orice material confidenţial al SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA transmis prin reţeaua Internet trebuie criptat.
13. Fişierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente şi regulamentele proprii fiecărui Departament.
14. Este interzisă accesarea site-urilor cu caracter pornografic
15. Este interzisă folosirea programelor peer-to-peer (exemple: Yahoo messenger, MSN, DC++, etc,)
16. Este interzisă descărcarea/instalarea programelor din reţeaua Internet

2.15. Administrarea Conturilor

Prin acord individual, fişa postului şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului RIC.

Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.

Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu **Regulamentul privind Parolele de Acces (cap.II subcap.2.16)**.

Conturile utilizator ale persoanelor plecate din Instituţie pe timp îndelungat (mai mult de 90 de zile) vor fi dezactivate (conturile nu vor mai putea fi accesate).

Toate conturile utilizator care nu au fost accesate timp de 30 de zile vor fi dezactivate. După încă 30 zile conturile vor fi şterse dacă nu s-a solicitat accesul la acestea.

Administratorii de sisteme sau alt personal autorizat sunt responsabili de ştergerea conturilor persoanelor (utilizatorilor) care nu mai lucrează în SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , sau care nu mai au relaţii cu SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .

2.16 Parole de Acces

1. Toate parolele trebuie să îndeplinească următoarele condiţii:
   - Să fie schimbate de utilizator în mod regulat, cel puţin o dată la 90 de zile;
   - Să aibă o lungime minimă de 6 caractere;
   - Să fie parole complexe;
   - Reutilizarea parolelor este interzisă;
   - Parolele stocate trebuie criptate;
   - Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice.
2. Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.
3. Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.

Utilizatorii nu pot folosi programe de stocare a parolelor. Se pot face excepţii pentru anumite aplicaţii (precum backup automat) cu aprobarea OSRIC.

Dispozitivele de calcul nu trebuiesc lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă.

Procedurile de schimbare a parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:

- Utilizatorul se va legitima, administratorul va verifica drepturile de acces a persoanei la contul utilizator;

- Se va genera o parolă care va fi comunicată utilizatorului

2.17 Sistemul de Mesagerie Electronică

Următoarele activităţi sunt interzise de regulament:

1. Trimiterea de mesaje cu caracter de intimidare sau hărţuire;
2. Folosirea sistemului de mesagerie electronică în scopuri personale;
3. Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
4. Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
5. Folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.
6. Folosirea programelor de poştă electronică neautorizate.
7. Următoarele activităţi sunt interzise deoarece împiedică buna funcţionare a comunicaţiilor în reţea şi eficienţa sistemelor de mesagerie electronică:
8. Trimiterea sau retrimiterea email-urilor în lanţ;
9. Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia.
10. Trimiterea mesajelor de dimensiuni foarte mari;
11. Trimiterea sau retrimiterea mesajelor ce pot conţine viruşi.
12. Toate informaţiile şi datele confidenţiale ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , transmise către alte reţele externe, trebuie să fie criptate.
13. Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea RIC ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA pot fi oricând înregistrate şi analizate.
14. Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că îşi spun opinia sau dau declaraţii în numele SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , cu excepţia situaţiilor în care aceştia sunt autorizaţi în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declaraţie explicită prin care utilizatorul specifică faptul că nu reprezintă SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA . Un exemplu de declaraţie simplă este: "părerile exprimate sunt personale, şi nu ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA" .
15. Utilizatorii nu trebuie să trimită, retrimită sau să primească informaţii confidenţiale sau senzitive ce privesc SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , folosind conturi utilizator care nu sunt proprietatea SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA . Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, AOL mail), precum şi adrese de email puse la dispoziţie de alţi Furnizorii de Servicii Internet.
16. Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informaţii confidenţiale sau nesigure, ce privesc SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , folosind dispozitive de comunicaţii mobile care nu sunt autorizate de SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA . Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenţi digitali personali, pagere ce permit trimiterea/primirea de informaţii şi telefoanele mobile.

2.18 Detectarea virusilor

1. Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , trebuie să utilizeze programe antivirus aprobate de către OSRIC.
2. Programele antivirus nu trebuie dezactivate.
3. Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.
4. Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.
5. Orice server de fişiere conectat la reţeaua Instituţiei trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curăţirii virusilor care pot infecta fişierele puse la dispoziţie.
6. Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat şi trebuie să respecte regulile de instalare şi utilizare a acestui program.
7. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat OSRIC sau OSRICD.

2.19 Licenţe de utilizare

1. SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA furnizează un număr suficient de copii cu Licenţă pentru toate programele aprobate spre utilizare astfel încât angajaţii să îşi poată desfăşura munca într-un mod eficient şi rapid.
2. SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA trebuie să se pună de acord în mod adecvat cu furnizorii implicaţi pentru obţinerea de copii adiţionale ale licenţelor dacă şi când acestea sunt necesare în activitatea instituţiei.
3. Copiile suplimentare ale materialelor protejate prin drepturi de autor nu vor fi stocate pe sistemele sau resursele reţelei SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA în situaţia în care nu există aprobări specifice. Administratorii de sistem vor şterge produsele şi toate materialele protejate prin drepturi de autor în situaţia menţionată, cu excepţia cazului în care utilizatorii implicaţi fac dovada autorizaţiei de folosire sau stocare de la producătorii de drept.
4. Programele sau alte bunuri informatice aflate sub incidenţa drepturilor de autor aflate în posesia SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA nu vor fi copiate, cu excepţia cazului în care această copiere este în concordanţă cu prevederile licenţei.

2.20 Relaţii cu terţi

Orice activitate desfăşurată de furnizor care implică acces la RIC trebuie să se conformeze cu regulamentele în vigoare ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
În toate convenţiile şi contractele încheiate cu Furnizori trebuie specificate următoarele:

- Informaţiile din cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , la care Furnizorul are drept de acces;
- Modul în care informaţiile la care Furnizorul are drept de acces urmează a fi protejate de către acesta precum şi măsuri ce vor fi luate în cazul nerespectării clauzelor;
- Metodele de predare, distrugere sau de transfer al drepturilor informaţiilor Instituţiei aflate în posesia Furnizorului, la încheierea contractului.
- Furnizorul trebuie să folosească sistemul RIC din cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA numai în scopul stipulat în contract.

- Orice altă informaţie din sistemul RIC al SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA obţinută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.
- Toate echipamentele de întreţinere ale Furnizorului, aflate în reţeaua internă a SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA şi care se pot conecta în exterior prin intermediul reţelei, a liniilor telefonice sau a liniilor închiriate, precum şi toate conturile de utilizator create temporar pentru Furnizor şi necesare pentru acces la RIC ale SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , vor fi scoase din uz la încheierea relaţiilor contractuale.
- Accesul Furnizorului trebuie să fie identificat în mod unic iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu **Regulamentul privind Parolele de Acces** (cap.II subcap.2.16) şi **Regulamentul de Acces Administrativ** (cap.II subcap.2.3).
- Activităţile principale ale Furnizorului trebuie să fie documentate de acesta şi puse la dispoziţia conducerii Instituţiei, la cerere. Acestea trebuie să cuprindă, dar să nu fie limitate la, evenimente precum: schimbări de personal, schimbări de parolă, schimbări majore în derularea proiectului, timpii de sosire, de plecare şi de livrare.
- În cazul retragerii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informaţiile sensibile sunt colectate şi predate SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA sau distruse în cel mult 24 de ore de la producerea evenimentului.
- În cazul terminării/rezilierii contractului sau la cererea SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , Furnizorul va preda sau distruge toate informaţiile ce aparţin Instituţiei şi va oferi certificare în scris privind predarea sau distrugerea informaţiilor în decurs de 24 de ore de la producerea evenimentului.
- În cazul încheierii contractului sau la cererea SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA , Furnizorul trebuie să predea imediat toate legitimaţiile, cartelele de acces, echipamentele şi stocurile SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA . Echipamentele şi/sau stocurile care urmează a fi reţinute de către Furnizor trebuiesc documentate şi autorizate de Conducerea SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA .
- Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA trebuie să fie inventariate corespunzător si să posede drepturi de utilizare atestate prin Licenţe.

Întocmit,
Ing. Cipriela BERINDEAN

VIZA DPO
Inf. Ana – Maria DADULESCU

Anexa 1

Istructiuni generale de lucru privind exploatarea Resurselor Informatice şi de Comunicaţii din cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA

- **Instructiune RIC_I.01** – Intervenţii în cazul defecţiunilor hardware;
- **Instructiune RIC_I.02** – Salvările de date, stocarea şi păstrarea acestora;
- **Instructiune RIC_I.03** – Achiziţii echipamente hardware şi/sau software pe bază de referat de necesitate, altele decât prin licitaţii;
- **Instructiune RIC_I.04** – Modificări sau defecţiuni ale aplicaţiilor software;
- **Instructiune RIC_I.05** – Exploatarea programelor informatice;
- **Instructiune RIC_I.06** – Activităţi de mentenanţă privind componentele harware;
- **Instructiune RIC_I.07** – Poşta electronică, sesizări pe site-ul primăriei, sesizări pe alte site-uri de specialitate;
- **Instructiune RIC_I.08** – Părăsirea temporara a calculatorului;
- **Instructiune RIC_I.09** – Atribuirea/schimbarea/anularea utilizatorilor şi a parolelor de access;

Instructiune RIC_I.01
Intervenţii în cazul defecţiunilor hardware

În cazul în care a fost constatată o defecţiune sau o disfuncţionalitate a vreunui sistem de calcul şi/sau a unui periferic al acestuia (monitor, tastatură, mouse, imprimantă, etc) se va informa OSRIC . Informarea se va face telefonic.

Poate exista şi cazul în care defecţiunea să fie constatată de către specialistul IT când acesta execută operaţiuni de întreţinere sau verificări de rutină.

Specialistul IT va constata în ce constă defecţiunea şi dacă este posibil va proceda la remedierea acesteia, in caz contrar se va anunţa OSRIC .

Instructiunea RIC_I.02
Salvările de date, stocarea şi păstrarea acestora

Salvările de date în general se fac pe suport magnetic extern (CD, memory stick), sau pe suport magnetic intern (hard disk) în funcţie de instrucţiunile existente în manualele programelor informatice. De asemenea perioada de păstrare a acestor salvări se va face tot în funcţie de aceste instrucţiuni. Dacă nu există instrucţiuni în acest sens păstrarea se va face pe perioadă nedeterminată.

În cazul salvărilor efectuate pe harddiskurile serverelor prin opţiunile existente în cadrul programelor informatice, se vor efectua salvari complete de către o persoană desemnată în acest sens de către ARIC la propunerea OSRIC.

Salvări complete ale harddiskurilor serverelor se va face de către specialistul IT / OSRIC din cadrul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA.

Pentru salvările efectuate şi pentru care nu există instrucţiuni privind termenul de păstrare a salvărilor, păstrarea se va face pe perioadă nedeterminată.

În cazul schimbări unui sistem informatic cu unul mai nou şi în care au fost preluate datele existente în salvările efectuate anterior, vechile salvări vor fi distruse.

Persoanele care efectuează salvări vor avea un jurnal de evidenţă al acestor salvări în care se va specifica clar data şi ora când a fost efectuată salvarea.

Instructiunea RIC_I.03
Achiziţii echipamente hardware şi/sau software pe bază de referat de necesitate, altele decât prin licitaţii

Pentru achiziţionarea echipamente hardware şi/sau software pe bază de referat de necesitate, referatul de necesitate înainte de a fi trimis spre aprobare conducerii instituţiei va fi avizat de către specialistul IT pentru a stabili dacă necesitatea achiziţionării echipamentelor este justificată sau nu. În cazul unui aviz favorabil referatul de necesitate va fi aprobat ulterior de către conducătorii instituţiei .

Referatele avizate şi aprobate vor fi transmise Compartimetului de achizitii pentru a fi achiziţionate echipamentele. Referatul va fi insotit de caietul de sarcini cuprinzand detaliile tehnice ale echipamentelor .

Recepţionarea acestora se va face respectând reglementarile interne specifice.

Instructiunea RIC_I.04
Modificări sau defecţiuni ale aplicaţiilor software

În cazul în care sunt necesare modificări ale aplicaţiilor software (programe informatice) în urma modificărilor legislative sau datorită altor cauze, sau constatării funcţionării defectoase, sau a apariţiei unor erori de funcţionare se va anunţa în scris sau telefonic,prin help-desk , prin email, sau prin fax, producătorul/autorul aplicaţiei sau firma care ofera asistenţă, după caz.

Departamentul care solicită modificările va furniza date cât mai amănunţite astfel încât modificările realizate să fie corecte.

Departamentul care solicită modificarea este răspunzător de datele furnizate.

Realizatorul modificărilor este răspunzător de modificările aduse în aplicaţia software. Acesta este obligat să informeze sau să instruiască utilizatorii aplicaţiilor despre modificările aduse.

În cazul defecţiunilor dacă se va constata că erorile de funcţionare se datorează unor defecţiuni ale echipamentului hardware se va anunţa specialistul IT şi se va urma procedura prevazuta in Instructiunea RIC_I.01.

Instructiune RIC_I.05
Exploatarea aplicatiilor informatice

Exploatare/utilizarea aplicaţiilor informatice se face doar de către personalul autorizat în conformitate cu instrucţiunile prevăzute în manualul aplicaţiei.

Utilizatorii noi care vor utiliza un program informatic vor fi instruiti de către persoanele abilitate în acest sens, de exemplu utilizatori cu vechime în exploatare acestuia sau de către un reprezentat al producătorului.

În cazul unui program informatic nou instruirea se face de către un reprezentant al producătorului programului informatic.

Dacă apar modificări din diverse motive se va urma Instructiunea RIC_I.04.

Instructiunea RIC_I.06

Activităţi de mentenanţă privind componentele hardware

Activităţi de mentenanţă privind componentele hardware se vor executa cel puţin o data pe lună la staţiile de lucru de către firma de service, iar pentru servere se va executa cel puţin o data pe săptămână de către specialistul IT / OSRIC şi o dată pe lună de către firma de service.

Verificările de rutină efectuate se vor evidenţia într-un jurnal de activităţi.

În cazul constatării unor nereguli în funcţionarea echipamentelor în urma acestor verificări se va urma Instructiunea RIC_I.01, privind intervenţiile în cazul defecţiunilor hardware.

Instructiunea RIC_I.07

Poşta electronică, sesizări pe site-ul primăriei, sesizări pe alte site-uri de specialitate

Mesajele sosite pe cale electronică: e-mailuri, sesizări postate site-ul SPITALULUI CLINIC DE RECUPERARE CLUJ NAPOCA (www.recuperarecluj.ro) sau sesizări postate pe alte site-uri de acest gen (ex. www.*medical*.ro), vor fi listate pe suport de hârtie şi depuse la registratura generală a instituţiei, după care vor fi direcţionate către departamentele de specialitate din cadrul instituţiei.

În cazul în care unele din aceste mesaje necesită răspuns, acesta va fi întocmit de către departamentele de specialitate din cadrul instituţiei si trimise spre aprobare conducerii **organizatiei**.

Instructiunea RIC_I.08

Părăsirea temporara a calculatorului. Oprirea Calculatorului

În cazul în care utilizatorul părăseşte temporar calculatorul este obligat să blocheze staţia de lucru prin utilizarea opţiunii **"Log Off"**, în cazul în care staţia este utilizată de mai mulţi utilizatori, sau prin utilizarea opţiunii **"Lock Computer"**. De asemenea este obligatorie selectarea opţiunii **"On resume, password protect"** din cadrul sectiunii **"Screen Saver".**

Este interzisă cu desăvârşire părăsirea staţiei de lucru fără a închide aplicaţiile în care se lucrează.

Instructiunea RIC_I.09

Atribuirea/schimbarea/anularea utilizatorilor şi a parolelor de access

Procedurile de schimbare a parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:

- Utilizatorul se va legitima, administratorul va verifica drepturile de acces a persoanei la contul utilizator;
- Se va genera o parolă care va fi comunicată utilizatorului
- Se va întocmi/actualiza fişa utilizatorului de către administrator.

În cazul în care un utilizator paraseşte definitiv sau temporar instituţia OSRIC va recurge la ştergerea contului acestei persoane.

Întocmit
Sef birou Informatica
Ing. Cipriela BERINDEAN

VIZA DPO
Inf. Ana-Maria DADULESCU

Uniunea Naţională a Barourilor din România
GIURGEA, GHIDRA
şi asociaţii
Societate civilă
de avocaţi