

SPITALUL DE BOLI PSIHICE CRONICE BORȘA

Capitolul 1. INTRODUCERE

În acord cu prevederile din prezentul regulament, Resursele Informatice și de Comunicații administrate de către Spitalul de Boli Psihice Cronice Borșa sunt bunuri strategice ale Spitalului, care trebuie administrate ca resurse ale statului român.

Compromiterea securității acestor resurse poate afecta capacitatea Spitalului de a oferi servicii informatice și de comunicații, poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilității instituției în fața partenerilor săi.

Prin urmare, prezentul regulament este motivat tehnic de necesitatea menținerii în funcțiune, în condiții de securitate, a rețelei informatice, precum și de necesitatea dezvoltării normale a unei resurse de informare.

1.1. Rețeaua informatică

Rețeaua de calculatoare a Spitalului cuprinde totalitatea Resurselor Informatice și de Comunicații ale unității, cu sau fără acces la rețeaua Internet/Intranet și are ca scop sprijinirea activității medicale prin mijloacele de comunicare și serviciile specifice oferite de rețelele de calculatoare conectate la Internet.

Orice activitate care se desfășoară prin intermediul rețelei trebuie să respecte legislația în vigoare (internă și internațională): *Legea nr. 64/2004, Legea nr. 285/2004, Legea nr. 451/2004, Legea nr. 496/2004, Legea nr. 51/2003, Legea nr. 161/2003, Legea nr. 196/2003, Legea 365/2002, Legea nr. 455/2001, Legea nr. 8/1996, HG nr. 1308/2002, Convenția privind Criminalitatea Informatică a Consiliului Europei, Declarația privind libertatea comunicării pe Internet a Consiliului Europei, etc.*), precum și prezentul Regulament.

1.2. Definiții și termeni

Internet = rețeaua internațională de calculatoare. Regulile acestei rețele se regăsesc în prevederile InterNIC, IPE.

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

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

Resurse Informatice și de Comunicații (RIC) = toate dispozitivele de tipărire/imprimare, dispozitive de afișare, unități de stocare și toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframeuri, servere, calculatoare personale, calculatoare-agendă (notebookuri, laptop-uri), calculatoare de buzunar, asistent digital personal (Personal Digital Assistant - PDA), pagere, sisteme de procesare distribuită, echipament de laborator și medical conectat la rețea și controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante și alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele și datele care sunt proiectate, construite, puse în funcțiune (operaționale) și menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afișa și transmite informația.

Utilizator = o persoană, o aplicație automatizată sau proces utilizator autorizat de către Spitalul de Boli Psihice Cronice Borșa, în conformitate cu procedurile și regulamentele în vigoare, să folosească Resursele Informatice și de Comunicații ale unității.

Abuz de privilegii = orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele unității și/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acțiunii respective.

Furnizor = persoană fizică/juridică care oferă bunuri sau servicii Spitalului de Boli Psihice Cronice Borșa în baza unui contract comercial sau de colaborare.

Capitolul 2. POLITICA DE SECURITATE

Politica de securitate este alcătuită astfel încât să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice publice, să stabilească practici prudente și acceptabile privind utilizarea RIC ale Spitalului și să instruiască utilizatorii care au dreptul de folosirea RIC privind responsabilitățile asociate unei astfel de utilizări.

2.1. Audiență

Politica de securitate a RIC ale Spitalului se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice RIC a instituției. Nu există nici un fel de conotații politice, religioase, rasiale legate de prevederile politicii de securitate. Trebuie privită doar ca un instrument de protecție a muncii utilizatorilor și nu ca un element restrictiv.

Prevederile Politicii vizează în mod direct utilizatorii rețelei spitalului, dar și furnizorii sau alte persoane, entități și organizații care au acces la RIC ale Spitalului.

2.2. Scop

Scopul urmărit de politica de securitate este acela de asigurare a integrității, confidențialității și disponibilității informației, precum și stabilirea cadrului necesar pentru elaborarea regulilor și procedurilor de securitate.

Confidențialitatea se referă la protecția datelor împotriva accesului neautorizat la fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea și sub controlul Spitalului, în condițiile legilor în vigoare.

Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la RIC.

Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor RIC. Diverse aplicații au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a RIC.

2.3. Clasificarea informațiilor

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

Pentru a asigura securitatea și integritatea informațiilor, acestea se împart în trei categorii principale:

Publice: Acestea sunt informațiile accesibile oricărui utilizator din interiorul sau exteriorul unității. Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra instituției sau aceste efecte sunt nesemnificative. Utilizatorii care furnizează aceste informații sunt responsabili de asigurarea integrității și disponibilității acestora în raport cu cerințele Spitalului.

Exemple: Informațiile de pe aviziere, servere web publice, știrile de presă, informările conducerii.

Secrete: În această categorie se includ informațiile care, datorită valorii economice și medicale, nu trebuie făcute publice. Se includ aici și informațiile pe care Spitalul trebuie să le protejeze conform legislației în vigoare. Datorită valorii economice și medicale asociate, aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate și distribuite în cadrul Spitalului doar utilizatorilor autorizați. Distribuirea acestor informații de către utilizatorii autorizați trebuie să se facă pe baza unei clauze de confidențialitate.

Exemple: clauze contractuale, conturi și parole folosite pe serverele de contabilitate sau gestiune
Strict Secrete sau Confidențiale: În această categorie se includ toate informațiile care, datorită valorii economice și medicale, nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidența Codului Civil, Penal sau legislației fiscale. Accesul la aceste

informații va fi restricționat. Datele strict secrete nu pot fi copiate, distribuite sau șterse fără acordul scris al conducerii unității.

Exemple: cheile criptografice, conturi administrative de pe serverele de gestiune, contabilitate, date medicale.

2.4. Atribuții și responsabilități

2.4.1. Atribuții manageriale

Orice angajat sau compartiment al Spitalului trebuie să se asigure că respectă prevederile prezentei Politici și a regulamentelor sau procedurilor asociate.

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

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

2.4.2. Atribuții și obligații ale administratorilor rețelei

Atribuțiile Administratorului rețelei au fost stabilite în baza contractului comercial pe care unitatea îl are încheiat cu scopul stabilirii în mod clar a responsabilității privind administrarea și buna funcționare a RIC din cadrul spitalului, precum și a responsabilității privind crearea, modificarea și aprobarea regulilor și politicilor referitoare la activitățile de administrare și utilizare a RIC.

Atribuțiile și obligațiile:

- Elaborarea și propunerea de modificări ale politicii de securitate a sistemului RIC;
- Elaborarea și propunerea pentru aprobare a planului de securitate (acesta conține o listă a tuturor regulilor și procedurilor de securitate aplicabile la sistemul de RIC;
- Elaborarea procedurilor pentru identificarea utilizatorilor RIC;
- Tratarea incidentelor de securitate în scopul minimizării efectului distructiv al acestora asupra RIC;
- Facilitarea evaluărilor legale, a cerințelor de tip „cele mai bune practici” pe măsură ce acestea devin recunoscute;
- Auditarea internă privind folosirea programelor pe toate componentele RIC;
- Elaborarea și actualizarea registrului riscurilor pentru RIC.

2.4.3. Atribuții și obligații ale utilizatorilor rețelei

Utilizatorii rețelei pot fi : medic, asistent medical, asistent social, psiholog, registrator medical, statistician, instructor ergoterapie, personal administrativ, colaboratori ai Spitalului care solicită calitatea de utilizator.

Utilizatorii standard nu au drept de administrare a rețelei și pot folosi numai acele RIC pentru care sunt autorizați, indiferent dacă sunt resurse locale sau resurse accesibile în Internet.

Atribuțiile și obligațiile utilizatorilor sunt următoarele:

- Să cunoască și să respecte prevederile politicii de securitate a RIC;
- Să cunoască și să respecte prevederile tuturor regulilor și procedurilor privind securitatea RIC (vezi *Anexe*);
- Să răspundă direct de securitatea și conținutul informațiilor și resurselor informatice și de comunicații încredințate direct sau indirect.

2.4.4. Alte atribuții

Toți partenerii Spitalului (furnizori, agenți, colaboratori, etc.) trebuie să accepte și să respecte politica de securitate, precum și regulile specifice privind utilizarea și securitatea RIC.

2.5. Prevederi pentru asigurarea integrității, confidențialității și disponibilității Informației în utilizarea RIC ale Spitalului de Boli Psihice Cronice Borșa

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

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

Întreg personalul este responsabil privind modul de utilizare a RIC și nu trebuie să facă abuz de privilegii; fiecare utilizator este direct responsabil pentru acțiunile care pot afecta securitatea RIC.

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

Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nu numai, mesagerie electronică, navigare Web, conversații telefonice, transmisie fax-uri și alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri, în condițiile legilor în vigoare.

Compartimentele sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC.

Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială și în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale și în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar.

Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația și datele sunt proprietatea Spitalului și trebuie să fie protejate.

Spitalul trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării RIC, protejării datelor și programelor împotriva întrebuintării greșite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat și controlat în mod corespunzător.

Orice program comercial utilizat în cadrul RIC trebuie să fie însoțit de Licență care să specifice clar drepturile de utilizare și restricțiile produsului. Personalul trebuie să respecte prevederile Licențelor și nu este permisă copierea ilegală a programelor comerciale. Unitatea își rezervă dreptul de a șterge orice produs fără licență de pe orice sistem din cadrul unității, precum și/sau fișier care nu are legătură cu scopul muncii respective.

Domeniul electronic www.spitalpsihiatricborsa.ro este gestionat de Spital ca domeniu propriu, în conformitate cu înregistrarea corespunzătoare a Spitalului ca proprietar al acestui domeniu, la autoritatea românească în materie de nume de domenii (RNC). Drepturile de utilizare ale acestui domeniului sunt rezervate pentru Spital.

Informațiile publicate electronic pe site-ul propriu www.spitalpsihiatricborsa.ro sunt proprietatea Spitalului de Boli Psihice Cronice Borșa. Caracterul public al acestora reflectă faptul că ele sunt puse la dispoziție în beneficiul comunității publice, în scop de informare asupra programelor și a activității Spitalului.

Orice utilizare a informațiilor de pe site-ul public al Spitalului în domeniul www.spitalpsihiatricborsa.ro, de către persoane particulare sau organizații, în alte scopuri decât cele în care au fost oferite, se face pe propria răspundere a acestora. Într-o asemenea eventualitate, Spitalul își rezervă dreptul de a solicita aplicarea prevederilor legale în vigoare.

Fișierele electronice create, trimise, primite sau stocate folosind RIC administrate sau în custodia și sub controlul Spitalului nu au caracter personal și pot fi accesate oricând de către angajații autorizați din cadrul Spitalului fără înștiințarea utilizatorului.

În scopul administrării RIC și pentru asigurarea securității acestora, personalul autorizat poate revizui sau utiliza orice informație stocată pe sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor (de exemplu: pagini web vizitate).

Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Spitalului, orice incident de posibilă întrebuintare greșită sau încălcare a acestui regulament (prin contactarea managerului unității).

Un mare număr de utilizatori pot accesa informații din exteriorul sistemului de comunicații al Spitalului. În aceste condiții, este obligatorie păstrarea confidențialității informațiilor transmise din exteriorul Spitalului și a informațiilor obținute din interiorul instituției. Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele Spitalului, pentru care nu au autorizație sau consimțământ explicit.

Nici un utilizator al RIC ale Spitalului nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemelor ce compun RIC. Această regulă se extinde și după ce utilizatorul a încheiat relațiile cu Spitalul.

Confidențialitatea informațiilor transmise prin intermediul resurselor de comunicații ale terților nu poate fi asigurată. Pentru aceste situații, confidențialitatea și integritatea informațiilor se poate

asigura folosind tehnici de criptare. Utilizatorii sunt obligați să se asigure că toate informațiile confidențiale ale Spitalului se transmit în așa fel încât să se asigure confidențialitatea și integritatea acestora.

Capitolul 3. PLANUL DE SECURITATE IT IN SPITALUL DE BOLI PSIHICE CRONICE BORȘA

3.1. Introducere

Planul de securitate conține toate regulile și procedurile aplicabile în sistemul RIC ale Spitalului.

Acestea sunt elaborate pentru a stabili un cadru corect, legal și eficient de utilizare a tehnologiei informației și comunicațiilor în Spital.

3.2. Scop

În acord cu legislația în vigoare în România și Regulamentele de ordine interioară ale Spitalului, RIC sunt valori ale acestuia care trebuie exploatate și administrate ca resurse publice în proprietatea statului român.

Planul de securitate are ca scop principal protejarea utilizatorilor și colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea, acesta are ca scop protejarea imaginii Spitalului, dezvoltarea sistemului informatic și de comunicații, protejarea proprietății intelectuale și a tuturor informațiilor stocate și transportate cu ajutorul RIC ale utilizatorilor autorizați.

Regulile (vezi *anexele prezentului Regulament*) au fost elaborate pentru fiecare activitate specifică domeniului și au fost concepute în așa fel încât, fiecare să poată fi folosită cvasiindependent de celelalte.

Regulile și procedurile din planul de securitate au rolul:

- de a fi corecte, echitabile și eficiente pentru folosirea RIC în vederea sprijinirii activității unității;
- de a educa utilizatorii RIC în ceea ce privește responsabilitățile asociate cu utilizarea acestora;
- de a fi compatibile cu regulamentele, statutul și atribuțiile stabilite pentru administrarea resurselor informatice și de comunicații.

3.3. Audiență

Regulile de utilizare a RIC ale Spitalului se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acestea.

3.4. Proceduri și Reguli specifice

Aceasta este lista tuturor regulilor sau procedurilor aplicabile în sistemul RIC:

1. Reguli de utilizare a RIC (*Anexa 1*)
2. Reguli privind accesul fizic la RIC (*Anexa 2*)
3. Reguli de acces la rețeaua de comunicații (*Anexa 3*)
4. Reguli de acces administrativ (*Anexa 4*)
5. Reguli privind configurarea sistemelor informatice pentru acces la rețeaua de comunicații (*Anexa 5*)
6. Reguli de tratare a incidentelor de securitate (*Anexa 6*)
7. Reguli de monitorizare a RIC (*Anexa 7*)
8. Reguli pentru detectarea accesului neautorizat (*Anexa 8*)
9. Reguli privind crearea și utilizarea copiilor de siguranță (*backup*) (*Anexa 9*)
10. Reguli de securizare a serverelor (*Anexa 10*)
11. Reguli privind securitatea informațiilor în cazul utilizării calculatoarelor portabile (*Anexa 11*)
12. Reguli pentru parolele de acces (*Anexa 12*)
13. Reguli de administrare a conturilor de email (*Anexa 13*)
14. Reguli privind sistemul de mesagerie electronică (*Anexa 14*)
15. Reguli de detectare a virusilor (*Anexa 15*)
16. Reguli de relații cu terți (*Anexa 16*)
17. Reguli pentru modificări și modernizări ale RIC (*Anexa 17*)
18. Procedură pentru alocarea unei adrese de email. Cerere tip (*Anexa 18*)
19. Procedură pentru conectarea la rețea. Cerere tip (*Anexa 19*)
20. Proces verbal de constatare (*Anexa 20*)
21. Exemple de activități interzise (*Anexa 21*)

Capitolul 4. MĂSURI DISCIPLINARE

Managerul unității are dreptul să ia măsuri de restricționare (blocare parțială sau totală), fără notificare, a accesului la RIC în cazul utilizatorilor care încalcă prevederile politicii de securitate și regulile aplicabile în sistemul de RIC (din planul de securitate) sau legislația în vigoare și care, astfel, pun în pericol funcționarea și/sau securitatea rețelei Spitalului.

În situații cu totul deosebite, când eventuale acțiuni ale unor utilizatori care, pe proprie răspundere, atentează grav la securitatea rețelei Spitalului, se pot lua următoarele măsuri:

- rezilierea contractului de muncă, în cazul angajaților;
- încetarea relațiilor contractuale (de colaborare), în cazul contractanților, furnizorilor sau consultanților.

Toate acțiunile care contravin legilor vor fi raportate organelor competente.

Capitolul 5. REFERINȚE

- Politica și Planul de securitate ale Spitalului ;
- *Legea nr. 455* din 18 iulie 2001 privind semnătura electronică;
- *Legea nr. 544* din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
- *Hotărârea nr. 1259* din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea *Legii nr. 455* din 2001 privind semnătura electronică;
- *Hotărârea nr. 781* din 25 iulie 2002 privind protecția informațiilor secrete de serviciu;
- *Legea nr. 182* din 12 aprilie 2002 privind protecția informațiilor clasificate;
- *Legea nr. 161* din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției.

Capitolul 6. DISPOZIȚII FINALE

Regulamentul va fi disponibil, împreună cu anexele, în format electronic pe site-ul web al Spitalului.

Prezentul document va conține informații de identificare proprii și se va specifica data la care a fost aprobat și data de la care intră în vigoare.

Modificarea prevederilor Regulamentului se face numai cu aprobarea conducerii Spitalului.

Manager
Ec. Ana Iucan



Director financiar-contabil
Ec. Elena Man



REGULI DE UTILIZARE a Resurselor Informatice și de Comunicații

A. Utilizarea permanentă a Resurselor Informatice și de Comunicații

1. Utilizarea RIC se face numai în interes de serviciu.
2. Utilizatorii trebuie să anunțe despre orice problemă/breșă în sistemul de securitate din cadrul Spitalului, cât și despre orice posibilă întrebuintare greșită sau încălcare a regulamentelor în vigoare.
3. Prin acțiunile lor, utilizatorii nu trebuie să încerce să compromită protecția sistemelor informatice 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 încerce să obțină acces la date sau programe din RIC pentru care nu au autorizație sau consimțământ 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 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 RIC; să împiedice accesul unui utilizator autorizat la RIC; 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 RIC. De exemplu, utilizatorii Spitalului nu trebuie să ruleze programe de decriptare a parolilor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.
10. RIC nu trebuie să fie folosite pentru beneficiul personal.
11. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe/care Spitalul le poate considera ofensive, indecente sau obscene.
12. Accesul la rețeaua Internet prin intermediul RIC se supune aceluiași regulamente care se aplică utilizării din interiorul instituției și Regulamentului pentru Utilizare Internet și Intranet.
13. Angajații nu trebuie să permită membrilor familiei sau altor persoane accesul la RIC ale Spitalului.
14. Utilizatorii care au acces la RIC ale Spitalului au obligația de a purta acte și/sau legitimații care să ateste calitatea de utilizator autorizat în spațiile instituției.
15. Utilizatorii vor folosi, exclusiv, numele de domeniu în toate activitățile desfășurate prin intermediul sau folosind RIC ale Spitalului.
16. Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor Spitalului folosind RIC.
17. Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Spitalului sau prejudicierea, indiferent de formă, a intereselor acestuia.
18. Toate mesajele, fișierele și documentele localizate în cadrul RIC sunt proprietatea Spitalului și pot fi subiectul unor cereri de verificare/inspectare/accesare conform regulamentelor.

B. Utilizarea ocazională a Resurselor Informatice și de Comunicații

În anumite situații este permisă utilizarea ocazională a RIC. În aceste situații se aplică următoarele restricții:

- utilizarea personală ocazională a serviciilor de poștă electronică, acces Internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricționată la utilizatorii autorizați și nu poate fi extinsă la membrii familiilor sau alte persoane;
- utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru Spital;
- utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaților.

**Reguli privind accesul fizic la Resursele Informatice și de Comunicații ale
Spitalului de Boll Psihice Cronice Borșa**

1. Toate sistemele de securitate fizică a RIC – cum ar fi, de exemplu: coduri de acces – trebuie să fie instalate în conformitate cu regulamentele Spitalului.
2. Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat și monitorizat.
3. Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcție de importanța acestora și tipul datelor vehiculate sau stocate.
4. Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RIC se aprobă accesul doar pentru personalul care răspunde de buna funcționare a echipamentelor din încăperea respectivă și, dacă este cazul, părților contractante, ale căror obligații contractuale implică acces fizic.
5. Personalul care are drepturi de acces trebuie să dețină legitimație de serviciu și acte de identitate care să-i ateste calitatea.
6. Acordarea drepturilor de acces (folosind chei, parole etc.) se face în scris, de către 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 raportate imediat.
10. Cheile nu trebuie să aibă informații de identificare.
11. Accesul vizitatorilor în spațiile protejate trebuie documentat pentru fiecare încăpere și, în cazul în care este permis, se va delega un însoțitor. Vizitatorii trebuie să fie însoțiți în zonele cu acces restricționat.
12. Compartimentul administrativ va ține o evidență a tuturor cheilor de acces emise, retrase, pierdute sau furate.
13. Pentru fiecare spațiu în care sunt instalate RIC se va păstra o evidență a accesului pentru verificări de rutină în situații critice.
14. Fiecare compartiment trebuie să verifice periodic drepturile de acces și să anuleze aceste drepturi pentru persoanele care pierd dreptul de acces.
15. 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 .

Reguli de acces la rețeaua de comunicații a Spitalului de Boli Psihice Cronice Borșa

1. Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la rețea specificați
2. **Conducerea** trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RIC ale Spitalului. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele și datele de identificare ale acesteia se vor comunica către administratorului sistemului .
3. Conectarea sistemelor de calcul care nu sunt proprietatea Spitalului se face numai cu aprobarea în scris a Managerului, la solicitarea sefilor de compartimente.
4. 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)) agreat de către Spital și folosind protocoale aprobate.
5. Utilizatorii RIC 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 la propunerea sefilor 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 să se conformeze cu standardele rețelei interne a Spitalului.
9. Utilizatorii nu au dreptul să descarce, să instaleze sau să ruleze programe de securitate care pot dezvălui slăbiciuni în securitatea unui sistem. De exemplu, utilizatorii Spitalului nu au dreptul să ruleze programe de spargere a parolei, 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 rețelei 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 plăci de rețea) fără aprobarea administratorului de rețea. Tipul și modelul plăcilor de rețea și tuturor echipamentelor care se pot conecta în rețea trebuie să fie aprobate de către administratorul de rețea .

Reguli de acces administrativ

1. Compartimentele spitalului trebuie să prezinte administratorului de rețea o listă cu informații de contact în plan administrativ pentru toate sistemele conectate la rețeaua de comunicații. Această listă trebuie refăcută și prezentată de fiecare dată când apar modificări de orice natură.
2. Utilizatorii trebuie să cunoască și să accepte toate regulamentele privind securitatea RIC înainte de a li se permite accesul la un cont.
3. Utilizatorii care au conturi de acces administrativ trebuie să aibă instrucțiuni de administrare, documentare, instruire și autorizare a conturilor. Aceste instrucțiuni se vor elabora de către fiecare compartiment și vor fi incluse în fișa postului.
4. Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activității pe care o desfășoară.
5. Accesul administrativ trebuie să se conformeze Regulilor pentru Parolele de acces. Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al administratorului de rețea și trebuie să fie schimbată atunci când persoana care utilizează acest cont își schimbă locul de muncă din cadrul Spitalului.
6. Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operațiuni definite. Acestea trebuie să îndeplinească următoarele condiții:
 - trebuie să fie autorizate;
 - trebuie create cu dată de expirare specifică;
 - contul va fi șters atunci când nu mai este necesar.

Anexa 5

Reguli privind configurarea sistemelor informatice pentru acces la rețeaua de comunicații

1. Infrastructura de comunicații, rețeaua de comunicații digitale a Spitalului este administrată de către administratorul de rețea care este responsabil cu întreținerea și dezvoltarea acesteia.
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 comunicații de date a Spitalului suportă un set definit de protocoale de rețea. Orice utilizare a altui set de protocoale 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 comunicații a Spitalului sunt responsabilitatea administratorului de rețea, conectarea se va face numai în baza unei cereri standard, aprobată de către managerul unității.
8. Toate conectările dintre rețeaua de comunicații a Spitalului și alte rețele de comunicații, publice sau private, sunt responsabilitatea exclusivă a administratorului de rețea.
9. Echipamentele de protecție a rețelei de comunicație a Spitalului (*firewall*) se vor instala de către administratorul de rețea.
10. Utilizatorii nu au dreptul să extindă sau să retransmită în niciun fel serviciile rețelei (este interzisă 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 de rețea sau programe care furnizează servicii de rețea, fără aprobarea conducerii.
12. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale rețelei.

Reguli de tratare a incidentelor de securitate

1. În cazul incidentelor de securitate din Spital, membrii conducerii Spitalului au funcții și responsabilități predefinite, care pot fi prioritare îndatoririlor obișnuite.
2. Ori de câte ori 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 înștiințarea și coordonarea pentru tratarea incidentului, strângerea dovezilor fizice și electronice ce vor face parte din documentația pentru tratarea incidentului.
5. Folosind resurse tehnice speciale se va monitoriza nivelul daunelor și gradul de eliminare sau atenuare a vulnerabilităților, acolo unde este cazul.
6. Administratorul rețelei, împreună cu managerul, stabilesc conținutul 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.
9. Administratorul rețelei este responsabil de coordonarea activităților de comunicare cu terții, pentru rezolvarea incidentului.
10. În cazul în care incidentul nu implică acțiuni contrare legilor în vigoare, administratorul rețelei va recomanda sancțiuni 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 acționa ca persoană de legătură cu acestea.

Anexa 7

Reguli de monitorizare a Resurselor Informatice și de Comunicații

Monitorizarea RIC se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice 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 protocoale și servicii) extern și conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat;
- Tipul protocoalelor și a echipamentelor conectate la RIC, conținutul 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 examinate regulat în vederea detectării eventualelor atacuri informatice 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 rețea;
- 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;
- Utilizării de modem-uri neautorizate;
- Licențelor pentru sistemele de operare și programelor instalate.

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

Anexa 8

Reguli pentru detectarea accesului neautorizat

1. Procesele de înregistrare și verificare a activității sistemelor de operare, conturilor utilizator și 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/revizuite (examine) zilnic de către administratorul de sistem sau trebuie instituit un sistem automatizat de avertizare.
5. Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această 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 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 conducerea unității.
10. Utilizatorii sunt obligați să raporteze conducerii și administratorului de sistem orice anomalii în performanța sistemelor utilizate sau orice semne ale unor posibile infracțiuni.

Anexa 9

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

1. Frecvența, dimensiunea și conținutul 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 RIC 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. Verificarea copiilor de siguranță se va face după o procedură documentată și revizuită periodic.
5. Copiile de siguranță trebuie să fie periodic testate pentru a asigura faptul că informațiile stocate sunt recuperabile.
6. Accesul la mediile de backup ale Spitalului, stocate la furnizori externi sau în interior se va face folosindu-se proceduri specifice de acces. Acestea trebuie revizuite periodic (anual). Accesul trebuie interzis pentru persoanele autorizate care își schimbă locul de muncă.
7. Benzile sau 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, incrementală, etc.);
 - clasificarea sensibilității (siguranței/securității);
 - informații de contact.

Reguli de securizare a serverelor

Un server va fi conectat la rețeaua Spitalului numai dacă se află într-o stare sigură, acreditată de către administratorul de rețea.

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 și a driver-elor care nu sunt necesare;
- Setarea/activarea parametrilor de securitate, a protecțiilor pentru fișiere și activarea jurnalelor de monitorizare;
- Dezactivarea sau schimbarea parolelor conturilor predefinite;
- Securizarea accesului fizic la aceste echipamente.

Administratorul de rețea va monitoriza, în mod obligatoriu, procesul de instalare a serverelor principale (enterprise) și aplicarea regulată a patch-urilor de securitate.

Anexa 11

Reguli privind securitatea informațiilor în cazul utilizării calculatoarelor 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 o altă alternativă de stocare locală, toate datele care privesc Spitalul trebuie criptate utilizând tehnici aprobate.
4. Transmiterea datelor prin rețele de tip wireless se poate face numai prin rețelele instalate de către administratorul de rețea; acestea vor utiliza tehnici de criptare pentru protejarea datelor transmise.
5. Toate accesările de la distanță a Resurselor Informatice și de Comunicații trebuie să se efectueze prin intermediul serviciului autorizat, conform *Regulilor de acces la rețeaua de comunicații (Anexa 3)*.
6. Conectarea sistemelor de calcul care nu sunt proprietatea Spitalului se face numai cu aprobarea scrisă a managerului unității.

Anexa 12

Reguli pentru parolele de acces

1. Orice parolă ar trebui să fie complexă și să aibă o lungime minimă de 8 caractere.

O parolă complexă este un șir de caractere compus din litere minuscule, majuscule, cifre și simboluri (%\$#&^* ...).

Criterii pentru stabilirea unei parole:

- nu este deloc recomandată folosirea simplă a datelor personale (ex: data nașterii, nume, prenume etc.) ca parole;
- folosiți cifre și simboluri ușor de asociat prin forma lor cu litere. De exemplu: a=@, B=8, E=3, i=1, l=! , O=0(zero), s=\$. *Exemplu: popescu1974 #p0p3\$cu#1974*
- faceți asocieri după ceva ce vă place: o carte, titlul unei melodii, titlul unui film, personajele dintr-un film, etc. și trasați-vă niște reguli de formare a parolei pe care să le folosiți de fiecare dată când aveți nevoie de o parolă nouă.

De exemplu: Prin asocierea inițialelor (să hotărâm că le vom folosi ca litere minuscule) titlului filmului „Pulp fiction” cu primele două litere din numele și prenumele personajelor *Vincent Vega* și *Mia Wallace*, folosind cifre și simboluri ușor de asociat cu litere (i=1, e=3, a=@), se poate obține parola: pfV1V3M1W@. Nu trebuie să vă străduiți foarte mult să țineți minte această parolă - care pare a fi complicată la prima vedere - pentru că o puteți deduce logic de fiecare dată când aveți nevoie de ea, important e să țineți minte regulile după care ați format-o.

2. Nu vă notați parolele pe hârtii.
3. Nu folosiți aceeași parolă pentru mai multe conturi.
4. Dacă aveți multe parole le puteți scrie într-un fișier, însă criptați acel fișier și asigurați-vă că nu-l veți pierde. Evitați denumirea celui fișier cu una explicită (*parolele mele.rar*).
5. Evitați să pastrați parole în agende electronice, telefoane mobile – pot fi furate.
6. Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puțin o dată la 90 de zile.
7. Aveți grijă la facilitatea browser-elor de reținere a parolelor (*AutoFill, Remember password*) cu atât mai mult atunci când calculatorul pe care lucrați e folosit de mai multe persoane.
8. Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaților care răspund de securitatea sistemelor informatice.
9. Dacă se suspectează că o parolă a putut fi divulgată, aceasta trebuie schimbată imediat.
10. Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.
11. Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă.
12. Schimbarea parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:
 - utilizatorul se va legitima;
 - administratorul va verifica drepturile de acces ale persoanei la contul utilizator;
 - utilizatorul va introduce o nouă parolă.

Anexa 13

Reguli de administrare a conturilor de email

1. Fiecare cont de email creat trebuie să aibă asociate o cerere și o aprobare corespunzătoare.
2. Toți utilizatorii sunt obligați 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. Toate parolele pentru conturi trebuie să fie create și folosite în conformitate cu *Regulile privind Parolele de Acces (Anexa 12)*.
5. Pentru păstrarea tuturor mesajelor primite este necesară instalarea unui client local de email (ex: *Mozilla Thunderbird, Outlook express* etc.) pe calculatorul individual al fiecărui utilizator.
6. La cererea conducerii, administratorul de rețea trebuie să furnizeze o listă cu toți utilizatorii (listă de conturi) pentru sistemele pe care le administrează.

Anexa 14

Reguli privind sistemul de mesagerie electronică

I. 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 altei identități decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.

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

- Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituția;
- Trimiterea sau retrimiterii mesajelor ce pot conține viruși;
- Ignorarea cererii administratorului rețelei de a elibera spațiile de pe server pe care le ocupă.

III. Alte mențiuni

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

- Toate activitățile utilizatorilor ce implică accesul și/sau folosirea resurselor informatice și de comunicații ale Spitalului pot fi oricând înregistrate și analizate.

- Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că își spun opinia sau dau declarații în numele Spitalului, cu excepția situațiilor în care aceștia sunt autorizați în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declarație explicită prin care utilizatorul specifică faptul că nu reprezintă Spitalul.

Un exemplu de declarație simplă este: "părerile exprimate sunt personale, și nu ale Spitalului ...".

- Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informații confidențiale sau nesigure, ce privesc Spitalul, folosind dispozitive de comunicații mobile care nu sunt autorizate de Spital. *Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: telefoane mobile, asistenți digitali personali, pagere ce permit trimiterea/primirea de informații.*

- Rețeaua Spitalului se declară a fi un mediu de lucru și comunicare academic, deschis și civilizat. Utilizatorii sunt invitați să se trateze reciproc în mod politicos și cordial. Spiritul Internet presupune dialoguri într-un stil caracterizat prin decență, amabilitate și bunăvoință. Partenerii noștri din Internet se așteaptă să găsească în Spital un mediu academic atunci când solicită informații despre noi, motiv pentru care, utilizatorii vor lua măsuri pentru a se autoidentifica corect atât pe serverul Spitalului, cât și în corespondența electronică pe care o trimit.

Anexa 15

Reguli de detectare a virusilor

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

5. Orice server de fișiere conectat la rețeaua instituției trebuie să utilizeze un program antivirus aprobat, în scopul detectării și curățirii virusilor care pot infecta fișierele puse la dispoziție.

6. 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.

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

Anexa 16

Reguli de relații cu terți

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 a fi protejate de către acesta, precum și măsuri ce vor fi luate în cazul nerespectării clauzelor;

- metodele de predare, distrugere sau de transfer al drepturilor informațiilor Spitalului aflate în posesia Furnizorului, la încheierea contractului.

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

3. Orice altă informație din sistemul RIC al Spitalului obținută 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 rețelei, precum și toate conturile de utilizator create temporar pentru Furnizor și necesare pentru acces la RIC ale Spitalului vor fi scoase din uz la încheierea relațiilor contractuale.

5. Accesul Furnizorului trebuie să fie identificat în mod unic, iar administrarea parolilor sau metodele de autentificare trebuie să fie în conformitate cu *Regulile privind parolele de acces* și *Regulile de acces administrativ*.

6. Activitățile principale ale Furnizorului trebuie să fie documentate de acesta și puse la dispoziția conducerii Spitalului, 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 și de livrare.

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

8. În cazul terminării/rezilierii contractului sau la cererea Spitalului, Furnizorul va preda sau distruge toate informațiile ce aparțin Spitalului și va oferi certificare în scris privind predarea sau distrugerea informațiilor în decurs de 24 de ore de la producerea evenimentului.

9. În cazul încheierii contractului sau la cererea Spitalului, Furnizorul trebuie să predea imediat toate legitimațiile, echipamentele și stocurile Spitalului. Echipamentele și/sau stocurile care urmează a fi reținute de către Furnizor trebuiesc documentate și autorizate de Conducerea Spitalului.

10. 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 Licențe.

Anexa 17

Reguli pentru modificări și modernizări ale RIC

Orice modificare asupra unei componente ale RIC din cadrul Spitalului (cum ar fi: sisteme de operare, componente hardware, echipamente și componente de rețea, aplicații) trebuie să respecte regulile de mai jos:

1. Toate modificările care afectează mediul de funcționare a sistemelor componente ale RIC (ex: aparate de aer condiționat, instalații de apă, încălzire, instalații electrice și alarme) trebuie să fie anunțate și aprobate în scris.

2. Toate propunerile de modernizare și extindere a elementelor de infrastructură a sistemului RIC vor fi documentate și aprobate de către conducere. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RIC.

3. Modificările și modernizările sistemelor de calcul vor fi documentate de către utilizator și aprobate de către conducere.

4. Modificările planificate trebuie anunțate cu cel puțin 48 ore înainte de a fi executate.

5. Cererile de modificare planificată pot fi respinse în următoarele cazuri: planificare inadecvată, planuri de refacere a serviciilor inadecvate, durata modificării poate afecta în mod negativ o activitate importantă a instituției sau resursele corespunzătoare necesare nu pot fi disponibile imediat.

6. Se va întocmi un raport pentru orice modificare, indiferent dacă a fost planificată sau neplanificată, sau dacă s-a realizat ori nu cu succes.

7. Trebuie întreținută o bază de date care să cuprindă toate modificările. Aceasta trebuie să conțină cel puțin următoarele informații:

- data la care s-a făcut cererea pentru modificare și data la care s-a făcut modificarea;
- informații de contact pentru utilizator;
- natura modificării;
- indicarea succesului sau nereușitei modificării.

Procedură pentru alocarea unei adrese de email. Cerere tip

Se adresează cadrelor medicale și personalului administrativ al Spitalului care doresc deschiderea unui cont de email pe domeniul **spitalpsihiatricborsa.ro**

1. Toti angajații au dreptul de a deține o adresă de email pe serverul Spitalului.
2. Se recomandă ca adresa de email să fie de forma: *nume@spitalpsihiatricborsa.ro* sau *prenume.nume@spitalpsihiatricborsa.ro* sau *inume@spitalpsihiatricborsa.ro* (unde i reprezintă inițiala prenumelui)
3. Cererile de obținere a unui cont de email pe serverul Spitalului este prezentată în modelul alăturat, se completează de către solicitant și se depune spre aprobare managerului.
4. Pentru verificarea căsuței poștale este pusă la dispoziție o interfață web la adresa <http://webmail.spitalpsihiatricborsa.ro>

Se poate accesa de pe orice calculator conectat la Internet, prin intermediul unui browser (*Mozilla Firefox, Internet Explorer, Google Chrome, Netscape Navigator, Opera, Safari, etc.*)

De asemenea, pe calculatorul fiecărui utilizator se va configura un client local de email (exemple: *Mozilla Thunderbird, Outlook express, Netscape Mail*).

Model cerere

CERERE DE DESCHIDERE A UNUI CONT DE EMAIL

Subsemnatul/a, _____
angajat al Spitalului de Boli Psihice Cronice Borșa în funcția de _____,
Compartimentul/Secția _____, telefon birou _____,
vă rog să-mi aprobați deschiderea unui cont de email pe domeniul *spitalpsihiatricborsa.ro*.
Numele de utilizator propus este: _____
(se recomandă folosirea numelui, eventual precedat de prenume sau de inițiala prenumelui).

Solicit ca mesajele primite pe acest cont de email să fie redirecționate automat :

Da, către adresa : _____
și doresc să păstrez mesajele și în contul deschis pe *spitalpsihiatricborsa.ro*: **Da** **Nu**
Nu

Prin semnarea acestui document mă angajez să respect *Regulamentul privind utilizarea și securitatea Resurselor Informatice și de Comunicații din cadrul Spitalului de Boli Psihice Cronice Borșa*.

Data: _____ Semnătura _____

Procedură pentru conectarea la rețea. Cerere tip

Se adresează cadrelor medicale și personalului din administrația Spitalului care doresc să se conecteze la rețeaua Internet a Spitalului.

1. Toate cadrele medicale și angajații care aparțin personalului administrativ pot solicita conectarea la rețeaua administrativă a Spitalului.

2. Cererea de conectare la rețeaua administrativă a Spitalului este prezentată în modelul alăturat, se completează de beneficiar și se depune spre aprobare managerului.

Observație:

Adresa fizică (MAC address) a calculatorului/laptop-ului pentru care se dorește conectarea la rețea se afla prin succesiunea de comenzi:

Start → Run (Search) → cmd → ipconfig -all

Adresa MAC este secvența numerică formată din 6 grupuri de câte 2 cifre hexadecimale (în baza 16) de tipul 00-0A-E4-A6-78-FB (*Physical Address* din secțiunea *Ethernet adapter Local Area Connection*).

Orice alte precizări necesare pentru conectarea la rețeaua Internet vor fi făcute beneficiarului la depunerea cererii.

3. În lipsa unei astfel de cereri echipamentele neautorizate se pot conecta la o rețea tip Musafir, dacă aceasta este disponibilă. Rețeaua tip Musafir permite accesul utilizatorilor la resurse din internet, dar nu permite accesul la resursele din rețeaua administrativă (Musafir -> any -> administrativ = deny all).

Model cerere

CERERE DE CONECTARE LA REȚEA

Subsemnatul/a, _____
angajat al Spitalului de Boli Psihice Cronice Borșa în funcția de _____,
Compartimentul/Secția _____, vă rog să-mi
aprobați conectarea la rețeaua internet a Spitalului a PC-ului/laptopului a cărui adresă fizică
(adresă MAC) este: _____.

Telefon birou: _____ Email: _____

Prin semnarea acestui document mă angajez să respect *Regulamentul privind utilizarea și securitatea Resurselor Informatice și de Comunicații* din cadrul Spitalului de Boli Psihice Cronice Borșa și să-l consult periodic pentru a fi la curent cu eventualele modificări survenite.

De asemenea, menționez că am luat la cunoștință faptul că nerespectarea acestuia poate duce la luarea unor măsuri de restricție a accesului meu la facilitățile rețelei de comunicații digitale a Spitalului de Boli Psihice Cronice Borșa.

Data: _____ Semnătura _____

Proces verbal de constatare

PROCES VERBAL DE CONSTATARE

Întocmit astăzi, ____ / ____ /20.., între:

- _____ administrator de sistem
 și
 - beneficiarul, _____, de la Departamentul _____
 (telefon: _____, email: _____)
 privind constatarea defecțiunilor echipamentului de mai jos.

Echipament:

Este în garanție : da.....nu.....

Defect reclamat:**Defect constatat:****Recomandări:**

Încheiat în două exemplare cu următoarea destinație: un exemplar rămâne în evidența administratorului de sistem, iar pe cel de-al doilea îl primește beneficiarul.

Exemple de activități interzise

Activități comerciale neautorizate:

- Trafic masiv de informații sau trafic de informații cu caracter frivol, obscen și pornografic;
- Folosirea unor drepturi de acces la resurse pentru care nu sunt autorizați;
- Ștergerea sau alterarea datelor altor utilizatori;
- Tentativele de descoperire și de folosire a parolilor altor utilizatori;
- Crearea sau folosirea de instrumente soft destinate spargerii sistemelor de securitate ale calculatoarelor;
- Provocarea deliberată de defecțiuni hardware și software;
- Perturbarea traficului rețelei Spitalului;
- Generarea de trafic neacademic;
- Transferuri de materiale care contravin legilor drepturilor de autor (software pirat, filme, muzică etc.);
- Generarea de spam;
- Jocuri online;
- Flood (indiferent de natura acestuia), de exemplu: ping flood;
- Răspândirea de aplicații de tip virus, troieni, viermi, spyware sau altele;
- Folosirea de aplicații de tip key-logere;
- Modificarea adresei MAC a plăcii de rețea;
- Setările pentru IP și DNS altfel decât cu "Obtain an IP/DNS address automatically";
- Utilizarea de programe pentru scanarea rețelei, exploit-uri;
- Realizarea de tunele;
- Transmiterea de mesaje cu caracter comercial;
- Publicitatea cu caracter comercial;
- Folosirea de software fără licență pe calculatoarele din Spital sau conectate la rețeaua Spitalului.

ANALIZA RISCURILOR SISTEMULUI IT

DIN CADRUL SPITALULUI DE BOLI PSHICE CRONICE BORȘA

Analiza riscului constituie un compartiment al abordării sistemice a luării deciziilor, realizării procedurilor și acțiunilor practice în procesul de soluționare a problemelor de avertizare (preîntâmpinare), ori de reducere a pericolului întreruperii funcționării sistemului informațional al Spitalului.

Esența gestiunii riscului se reduce la colectarea și analiza informațiilor privind funcționarea sistemului informațional în ansamblu și a fiecărei componente a lui, la analiza riscului (pericolului) și controlului funcționării sistemului de securitate informațională.

Procedura analizei riscului este parte componentă a planului de securitatea IT implementat la nivelul Spitalului, analizei economice în baza criteriilor "valoare-securitate-profit"; asigurării și a altor categorii de analize și estimare a situației securității sistemului informațional.

Sarcina de bază a analizei riscului constă în oferirea informațiilor obiective privind funcționarea sistemului informațional pentru acele persoane, care preiau decizii referitoare la securitatea celui de pe urmă.

În acest sens, analiza examinată trebuie să formuleze răspunsuri la următoarele trei întrebări de bază:

1. Ce rău se poate produce? (identificarea pericolului)
2. Cât de frecvent aceasta poate să se întâmple? (analiza frecvenței)
3. Care pot fi consecințele? (analiza consecințelor)

De asemenea analiza în cauză poate fi considerată drept remediu eficace, în cadrul și grație căreia sunt determinate modalitățile de abordare a depistării pericolelor și riscurilor, se întreprind acțiuni de formulare a deciziilor obiective referitor la nivelul riscului posibil, la stabilirea exigențelor și recomandărilor privind reglarea securității examinate.

Sunt posibile mai multe variante ale strategiei securității funcționării sistemului informațional (S.I.) în condiții de luare a deciziilor în situații de incertitudine, dar de bază sunt următoarele trei:

1. Prima variantă constă în **evitarea riscului**. Ea se reduce la refuz de acțiuni ce ar conduce la anumit risc, precum și din temeri de consecințe defavorabile și din motiv că cele întreprinse în principiu nu pot avea loc în procesul funcționării S.I. De exemplu, chiar și în S.I. local închis efectiv poate exista riscul pierderilor de informații provocate de intervenții ale utilizatorilor atât la nivel fizic, cât și logic și semantic. Pe lângă aceasta, e necesar de ținut cont de faptul, că S.I. încorporează o mulțime considerabilă de componente, care dispun de colecții de diverși parametri tehnici (timpul prelucrării refuzului, probabilitatea refuzului ș.a.).
2. A doua variantă este **acceptarea riscului**. Această strategie este legată de faptul că administratorul, în mod conștient, recurge la risc până atunci când consecințele riscurilor ce s-au produs nu vor conduce la pierderi irecuperabile. Varianta examinată nu poate fi considerată optimală, așa acum nu exclude consecințe fatale.
3. A treia variantă a strategiei securității S.I. se reduce la **gestiunea riscului**. Ea constă în determinarea și estimarea, precum și elaborarea acțiunilor (măsurilor) minimizării riscului. De menționat că gestiunea riscurilor este un domeniu interdisciplinar specific, care solicită cunoștințe fundamentale referitoare la teoria sistemelor complexe (compuse), teoria protecției informației ș.a.

În această situație e necesar să fie elaborată o strategie de gestiune a riscurilor de diverse clase, în baza următoarelor modalități de abordare:

- **diminuarea riscului** prin aplicarea remediilor simple și accesibile, cum ar fi de exemplu, organizarea rațională a gestiunii parolelor utilizatorilor, care de cele mai multe ori reduce pericolul accesului nesancționat;
- **evaziune de la risc** prin intermediul acțiunilor de ordin organizatoric;
- **schimbarea caracterului riscului** pe contul funcției asigurării în cazurile apariției situațiilor imprevizibile;
- **acceptarea riscului** contând pe strategia gestiunii lui.

Strategia gestiunii riscului, de asemenea, depinde și de varietatea și indicatorii cantitativi ai acestuia.

Actualmente sunt cunoscute următoarele varietăți de riscuri și indicatori ce-i caracterizează:

- **risc individual** – caracterizat în baza unui indicator cum ar fi frecvența defectării unei componente a sistemului (de exemplu: calculatorul, sistemul de operare, aplicația programată, baza de date ș.a.) provocată de influența anumitor factori de pericol;
- **risc colectiv** - se caracterizează prin numărul întreruperilor (penelor) previzibile pe parcursul unui anumit termen temporal (de exemplu: refuz în deservire, pierderea resurselor informaționale ș.a.);
- **risc potențial** – caracterizat prin distribuirea spațială a frecvenței influenței negative de anumit nivel asupra sistemului;
- **risc social** - caracterizat de frecvența evenimentelor negative, în urma cărora au suferit utilizatorii sistemului.

Procesul de gestiune a riscului poate fi realizat de următoarele acțiuni efectuate în următoarea succesiune:

- evidențierea riscului ipotetic;
- estimarea riscului;
- selectarea metodelor de gestiune a riscului;
- aplicarea metodelor selectate;
- estimarea rezultatelor.

Baza metodologică de realizare a analizei riscului include în sine următorii pași efectuați în următoarea succesiune:

Pasul 1 - Determinarea și descrierea tuturor activelor sistemului informațional, printre ele de bază fiind hard-ul, soft-ul și datele. Totodată, se stabilește valoarea nominală a acestor active cu luarea în considerație a termenului de exploatare, valorii de restituire (înlocuire) și alte criterii subiective.

Pasul 2 - Formarea listei amenințărilor posibile și probabile. Drept amenințare se consideră orice acțiune, care ar provoca deschideri neautorizate, distrugerii, modificări și refuz de deservire. Prin urmare, în cadrul acestei etape are loc identificarea mulțimii de amenințări, cu concretizarea cât mai satisfăcătoare a probabilității (frecvenței) lor și a pierderilor așteptate.

Pasul 3 - Calcularea dimensiunilor pierderilor posibile în cazul producerii amenințărilor probabile.

Pasul 4 - Determinarea remediilor posibile de opunere și verificarea amenințărilor, evidențierea remediilor, costurilor și eficienței lor.

Pasul 5 - Calcularea și determinarea rezultatelor financiare, obținute de la realizarea fiecărui remediu de opunere amenințărilor, prin contrapunerea cheltuielilor și profitului de la efectuarea lor.

Pasul 6 - Determinarea și formularea recomandărilor privind selectarea remediilor de opunere și de verificare a amenințărilor. În cazul selecției metodelor de opunere și verificare a acestor amenințări e necesar de ținut cont de tipul S.I., caracterul amenințărilor (posibile și potențiale), scopurile analizei, criteriile riscului admisibil, dispunerea de resurse necesare pentru efectuarea analizei, de informații respective, de experiența și calificarea executorilor ș.a.

După scopurile urmărite amenințările pot fi sistematizate în următoarele categorii:

- violarea integrității informațiilor;
- violarea accesibilității informațiilor ori capacității de funcționare a sistemului ;
- violarea confidențialității informațiilor; informațiile păstrate și prelucrate de sistem;
- violarea valorii și semnificației juridice a informațiilor.

