REGULAMENT DE SECURITATE IT

SPITALUL DE BOLI PSIHICE CRONICE BORȘA

Capitolul 1. INTRODUCERE

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

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

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

1.1. Reţeaua informatică

Reţeaua de calculatoare a Spitalului cuprinde totalitatea Resurselor Informatice şi de Comunicaţie ale unităţii, cu sau fără acces la reţeaua Internet/Intranet și are ca scop sprijinirea activităţii medicale prin mijloacele de comunicare şi serviciile specifice oferite de reţelele de calculatoare conectate la Internet.

Orice activitate care se desfăşoară prin intermediul reţelei trebuie să respecte legislaţia în vigoare (internă şi internaţională): *Legea nr. 64/2004, Legea nr. 285/2004, Legea nr.451/2004, Legea nr. 496/2004, Legea nr. 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, Convenţia privind Criminalitatea Informatică a Consiliului Europei, Declaraţia privind libertatea comunicării pe Internet a Consiliului Europei, etc.)*, precum şi prezentul *Regulament.*

1.2. Definiţii şi termeni

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

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

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

Resurse Informatice şi de Comunicaţii (RIC) = toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: 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 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 crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.

Utilizator = o persoană, o aplicaţie automatizată sau proces utilizator autorizat de către Spitalul de Boli Psihice Cronice Borșa, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicaţii ale unităţii.

Abuz de privilegii = orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele unităţii şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.
Furnizor = persoană fizică/juridică care oferă bunuri sau servicii 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 şi alte documente oficiale în vigoare privind administrarea resurselor informatice publice, să stabilească practici prudente şi acceptabile privind utilizarea RIC ale Spitalului şi să instruiască utilizatorii care au dreptul de folosirea RIC privind responsabilităţile asociate unei astfel de utilizări.

2.1. Audienţă

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

Prevederile Politicii vizează în mod direct utilizatorii reţelei spitalului, dar şi furnizorii sau alte persoane, entităţi şi organizaţii care au acces la RIC ale Spitalului.

2.2. Scop

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

Confidenţialitatea se referă la protecţia datelor împotriva accesului neautorizat la fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea şi sub controlul Spitalului, în condiţiile legilor în vigoare.
Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la RIC .

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

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

2.3. 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: Acestea sunt informaţiile accesibile oricărui utilizator din interiorul sau exteriorul unităţii. Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra instituţiei sau aceste efecte sunt nesemnificative. Utilizatorii care furnizează aceste informaţii sunt responsabili de asigurarea integrităţii şi disponibilităţii acestora în raport cu cerinţele Spitalului.
Exemple: Informaţiile de pe aviziere, servere web publice, ştirile de presă, informările conducerii .

Secrete: În această categorie se includ informaţiile care, datorită valorii economice și medicale, nu trebuie făcute publice. Se includ aici şi informaţiile pe care Spitalul trebuie să le protejeze conform legislaţiei în vigoare. Datorită valorii economice și medicale asociate, aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate şi distribuite în cadrul Spitalului doar utilizatorilor autorizaţi. Distribuirea acestor informaţii de către utilizatorii autorizaţi trebuie să se facă pe baza unei clauze de confidenţialitate.
Exemple: clauze contractuale, conturi și parole folosite pe serverele de contabilitate sau gestiune

Strict Secrete sau Confidenţiale: În această categorie se includ toate informaţiile care, datorită valorii economice și medicale, nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidenţa Codului Civil, Penal sau legislaţiei fiscale. Accesul la aceste

informaţii va fi restricţionat. Datele strict secrete nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii unităţii.
Exemple: cheile criptografice, conturi administrative de pe serverele de gestiune, contabilitate, date medicale.

2.4. Atribuţii şi responsabilităţi

2.4.1. Atribuţii manageriale

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

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

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

2.4.2. Atribuţii şi obligaţii ale administratorilor reţelei

Atribuţiile Administratorului reţelei au fost stabilite în baza contractului comercial pe care unitatea îl are încheiat cu scopul stabilirii în mod clar a responsabilităţii privind administrarea şi buna funcţionare a RIC din cadrul spitalului, precum şi a responsabilităţii privind crearea, modificarea şi aprobarea regulilor şi politicilor referitoare la activităţile de administrare şi utilizare a RIC.

Atribuţiile şi obligaţiile:

- Elaborarea şi propunerea de modificări ale politicii de securitate a sistemului RIC;
- Elaborarea şi propunerea pentru aprobare a planului de securitate (acesta conţine o listă a tuturor regulilor şi procedurilor de securitate 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 cerinţelor de tip „cele mai bune practici" pe măsură ce acestea devin recunoscute;
- Auditarea internă privind folosirea programelor pe toate componentele RIC;
- Elaborarea şi actualizarea registrului riscurilor pentru RIC.

2.4.3. Atribuţii şi obligaţii ale utilizatorilor reţelei

Utilizatorii reţelei 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 reţelei şi pot folosi numai acele RIC pentru care sunt autorizaţi, indiferent dacă sunt resurse locale sau resurse accesibile în Internet.

Atribuţiile şi obligaţiile utilizatorilor sunt următoarele:

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

2.4.4. Alte atribuţii

Toţi partenerii Spitalului (furnizori, agenţi, colaboratori, etc.) trebuie să accepte şi să respecte politica de securitate, precum şi regulile specifice privind utilizarea şi securitatea RIC.

2.5. Prevederi pentru asigurarea integrităţii, confidenţialităţii şi disponibilităţii Informaţiei în utilizarea RIC ale Spitalului de Boli Psihice Cronice Borşa

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

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

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

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

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

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

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

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

Spitalul trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIC, protejării datelor şi programelor împotriva întrebuinţării greşite, în concordanţă cu necesităţile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător.

Orice program comercial utilizat în cadrul RIC trebuie să fie însoţit de Licenţă care să specifice clar drepturile de utilizare şi restricţiile produsului. Personalul trebuie să respecte prevederile Licenţelor si nu este permisă copierea ilegală a programelor comerciale. Unitatea îşi rezervă dreptul de a şterge orice produs fără licenţă de pe orice sistem din cadrul unităţii, precum și/sau fişier care nu are legătură cu scopul muncii respective.

Domeniul electronic www.spitalpsihiatrieborsa.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.

Informaţiile publicate electronic pe site-ul propriu www.spitalpsihiatrieborsa.ro sunt proprietatea Spitalului de Boli Psihice Cronice Borșa. Caracterul public al acestora reflectă faptul că ele sunt puse la dispoziţie în beneficiul comunităţii publice, în scop de informare asupra programelor şi a activităţii Spitalului.

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

Fişierele electronice create, trimise, primite sau stocate folosind RIC administrate sau în custodia şi sub controlul Spitalului nu au caracter personal şi pot fi accesate oricând de către angajaţii autorizaţi din cadrul Spitalului fără înştiinţarea utilizatorului.

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

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

Un mare număr de utilizatori pot accesa informaţii din exteriorul sistemului de comunicaţii al Spitalului. În aceste condiţii, este obligatorie păstrarea confidenţialităţii informaţiilor transmise din exteriorul Spitalului şi a informaţiilor obţinute din interiorul instituţiei. Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Spitalului, pentru care nu au autorizaţie sau consimţământ explicit.

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

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 se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

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

3.1. Introducere

Planul de securitate conţine toate regulile şi procedurile aplicabile în sistemul RIC ale Spitalului.

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

3.2. Scop

În acord cu legislaţia în vigoare în România şi 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 şi colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea, acesta are ca scop protejarea imaginii Spitalului, dezvoltarea sistemului informatic şi de comunicaţii, protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate cu ajutorul RIC ale utilizatorilor autorizaţi .

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

Regulile şi procedurile din planul de securitate au rolul:
- de a fi corecte, echitabile şi eficiente pentru folosirea RIC în vederea sprijinirii activităţii unităţii;
- de a educa utilizatorii RIC în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;
- de a fi compatibile cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

3.3. Audienţă

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

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

Capitolul 4. MĂSURI DISCIPLINARE

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

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

- rezilierea contractului de muncă, în cazul angajaţilor;
- încetarea relaţiilor contractuale (de colaborare), în cazul contractanţilor, furnizorilor sau consultanţilor.

Toate acţiunile care contravin legilor vor fi raportate organelor competente.

Capitolul 5. REFERINŢE

- Politica şi Planul de securitate ale Spitalului ;
- *Legea nr. 455* din 18 iulie 2001 privind semnătura electronică;
- *Legea nr. 544* din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
- *Hotărârea nr. 1259* din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea *Legii nr. 455* din 2001 privind semnătura electronică;
- *Hotărârea nr. 781* din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu;
- *Legea nr. 182* din 12 aprilie 2002 privind protecţia informaţiilor clasificate;
- *Legea nr. 161* din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei.

Capitolul 6. DISPOZIŢII FINALE

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

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

Modificarea prevederilor Regulamentului se face numai cu aprobarea conducerii Spitalului.

Anexa 1

REGULI DE UTILIZARE
a Resurselor Informatice şi de Comunicaţii

A. Utilizarea permanentă a Resurselor Informatice şi de Comunicaţii

1. Utilizarea RIC se face numai în interes de serviciu.
2. Utilizatorii trebuie să anunţe despre orice problemă/breşă în sistemul de securitate din cadrul Spitalului, cât şi despre orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.
3. Prin acţiunile lor, utilizatorii 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.
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 si 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 hărţui sau ameninţa alte persoane; să degradeze performanţele sistemelor ce alcătuiesc 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.
9. Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii sistemelor ce alcatuiesc RIC. De exemplu, utilizatorii Spitalului 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 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 reţeaua Internet prin intermediul RIC se supune aceloraşi regulamente care se aplică utilizării din interiorul instituţiei şi Regulamentului pentru Utilizare Internet şi Intranet.
13. Angajaţii nu trebuie să permită membrilor familiei sau altor persoane accesul la RIC ale Spitalului
14. Utilizatorii care au acces la RIC ale Spitalului au obligaţia de a purta acte şi/sau legitimaţii care să ateste calitatea de utilizator autorizat în spaţiile instituţiei.
15. Utilizatorii vor folosi, exclusiv, numele de domeniu în toate activităţile desfăşurate prin intermediul sau folosind RIC ale Spitalului .
16. Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor Spitalului folosind RIC.
17. Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale impotriva Spitalului sau prejudicierea, indiferent de formă, a intereselor acestuia.
18. Toate mesajele, fişierele şi documentele localizate în cadrul RIC sunt proprietatea Spitalului şi pot fi subiectul unor cereri de verificare/inspectare/accesare conform regulamentelor.

B. Utilizarea ocazională a Resurselor Informatice şi de Comunicaţii

În anumite situaţii este permisă utilizarea ocazională a RIC. În aceste situaţii se aplică următoarele restricţii:

- utilizarea personală ocazională a serviciilor de poştă electronică, acces Internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricţionată la utillizatorii autorizaţi şi 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 angajaţilor.

Anexa 2

Reguli privind accesul fizic la Resursele Informatice şi de Comunicaţii ale Spitalului de Boli Psihice Cronice Borşa

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 şi monitorizat.
3. Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi 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 funcţionare a echipamentelor din încăperea respectivă şi, dacă este cazul, părţilor contractante, ale căror obligaţii contractuale implică acces fizic.
5. Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.
6. Acordarea drepturilor de acces (folosind chei, parole etc.) se face în scris, de către conducerea unităţii.
7. Nu este permis transferul dreptului de acces indiferent de motiv.
8. Cheile de acces care nu mai sunt folosite trebuie predate comnpartimentului care le-a eliberat.
9. Pierderea sau furtul cheilor de acces trebuie raportate imediat.
10. Cheile nu trebuie să aibă informaţii de identificare.
11. Accesul vizitatorilor în spaţiile protejate trebuie documentat pentru fiecare încăpere şi, în cazul în care este permis, se va delega un însoţitor. Vizitatorii trebuie să fie însoţiţi în zonele cu acces restricţionat.
12. Compartimentul administrativ va ţine o evidenţă a tuturor cheilor de acces emise, retrase, pierdute sau furate.
13. Pentru fiecare spaţiu în care sunt instalate RIC se va păstra o evidenţă a accesului pentru verificări de rutină în situaţii critice.
14. Fiecare compartiment trebuie să verifice periodic drepturile de acces şi să anuleze aceste drepturi pentru persoanele care pierd dreptul de acces.
15. Fiecare compartiment trebuie să anuleze drepturile de acces al cheilor utilizatorilor care îşi schimbă locul de muncă din Spital sau nu au relaţii contractuale cu Spitalul .

Anexa 3

Reguli de acces la reţeaua de comunicaţii a Spitalului de Boli Psihice Cronice Borşa

1. Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi
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 şi 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 distanţă la reţeaua Spitalului se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către Spital şi folosind protocoale aprobate.
5. Utilizatorii RIC din interiorul Spitalului nu se pot conecta la altă reţea.
6. Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în niciun fel, pe nici o cale. Nu este permisă instalarea de conexiuni de reţea 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 reţea, fără aprobarea conducerii.
8. Sistemele computerizate din afara Spitalului care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei 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 conectaţi la reţeaua Spitalului.
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 administratorul de retea.
12. Serviciile de interconectare a reţelei Spitalului cu alte reţele sunt realizate exclusiv de către administratorul de retea.
13. Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea administratorul de retea. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către administratorul de retea .

Anexa 4

Reguli de acces administrativ

1. Compartimentele spitalului trebuie să prezinte administratorului de retea o listă cu informaţii de contact în plan administrativ pentru toate sistemele conectate la reţeaua de comunicaţii. Această listă trebuie refăcută şi prezentată de fiecare dată când apar modificări de orice natură.
2. Utilizatorii trebuie să cunoască şi 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 sa aibă instrucţiuni de administrare, documentare, instruire şi autorizare a conturilor. Aceste instrucţiuni se vor elabora de către fiecare compartiment şi vor fi incluse în fişa postului.
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 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 retea şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi 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 operaţiuni definite. Acestea trebuie să îndeplinească următoarele condiţii:
- trebuie să fie autorizate;
- trebuie create cu dată de expirare specifică;
- contul va fi şters atunci când nu mai este necesar.

Anexa 5

Reguli privind configurarea sistemelor informatice pentru acces la reţeaua de comunicaţii

1. Infrastructura de comunicaţii, reţeaua de comunicaţii digitale a Spitalului este administrată de către administratorul de retea 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 administratorul de retea. Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor administratorului de retea.
3. Orice dispozitiv hardware, inclusiv plăcile de reţea, care se va conecta la reţeaua Spitalului, trebuie să fie însoţit de o aprobare de tip (producător, model, etc.) din partea administratorului de retea.
4. Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai de catre administratorul de retea.
5. Infrastructura de comunicaţii de date a Spitalului suportă un set definit de protocoale de reţea. Orice utilizare a altui set de protocoale se face de către administratorul de reţea.
6. Adresele de reţea sunt alocate dinamic sau static numai de către administratorul de retea.
7. Toate conectările în reţeaua de comunicaţii a Spitalului sunt responsabilitatea administratorul de retea, conectarea se va face numai în baza unei cereri standard, aprobată de către managerul unităţii.
8. Toate conectările dintre reţeaua de comunicaţii a Spitalului şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a administratorului de retea.
9. Echipamentele de protecţie a reţelei de comunicaţie a Spitalului (*firewall*) se vor instala de către administratorul de retea.
10. Utilizatorii nu au dreptul să extindă sau să retransmită în niciun fel serviciile reţelei (este interzisă instalarea unui fax, modem, router, switch, hub sau punct de acces la reţeaua Spitalului) fără aprobare din partea conducerii.
11. Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau programe care furnizează servicii de reţea, fără aprobarea conducerii.
12. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

Anexa 6

Reguli de tratare a incidentelor de securitate

1. În cazul incidentelor de securitate din Spital, membrii conducerii Spitalului au funcţii şi responsabilităţi predefinite, care pot fi prioritare îndatoririlor obişnuite.
2. Ori de câte ori un incident de securitate este suspectat sau confirmat (exemple: virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate, etc.), trebuie urmate procedurile standard specifice pentru micşorarea riscurilor.
3. Administratorul retelei este responsabil cu înştiinţarea şi coordonarea pentru tratarea incidentului, strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului.
5. Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităţilor, acolo unde este cazul.
6. Administratorul retelei, împreună cu managerul, stabilesc conţinutul comunicatelor pentru utilizatori privind incidentele şi vor determina nivelul şi modul de distribuire a acestor informaţii.
7. Administratorul retelei trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.
8. Administratorul retelei este responsabil cu documentarea anchetei privind incidentul.
9. Administratorul retelei este responsabil de coordonarea activităţilor de comunicare cu terţii, pentru rezolvarea incidentului.
10. În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare, administratorul retelei va recomanda sancţiuni disciplinare.
11. În cazul în care incidentul implică aplicarea legilor civile sau penale, administratorul retelei va recomanda managerului sesizarea organelor în drept ale statului şi va acţiona ca persoană de legătură cu acestea.

Anexa 7

Reguli de monitorizare a 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 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. În această categorie intră următoarele (fără a se limita doar la acestea):
- Jurnale ale sistemelor de detectare automată a intruşilor;
- Jurnale Firewall;
- Jurnale ale activităţii conturilor utilizator;
- Jurnale ale scanărilor reţea;
- Jurnale ale aplicaţiilor;
- Jurnale ale solicitărilor de suport tehnic;
- Jurnale ale erorilor din sisteme şi servere.

Administratorul retelei va efectua, în mod regulat (cel puţin o dată la şase luni), verificări pentru detectarea:
- Echipamentelor de reţea conectate neautorizat;
- Serviciilor de reţea neautorizate;

- Serverelor de pagini de web neautorizate;
- Echipamentelor ce utilizează resurse comune nesecurizate;
- Utilizării de modem-uri neautorizate;
- Licenţelor pentru sistemele de operare şi programelor instalate.

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

Anexa 8

Reguli pentru detectarea accesului 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 sau trebuie instituit un sistem automatizat de avertizare.
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 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 unităţii .
10. Utilizatorii sunt obligaţi să raporteze conducerii și administratorului de sistem orice anomalii în performanţa sistemelor utilizate sau orice semne ale unor posibile infracţiuni.

Anexa 9

Reguli privind 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. Procedurile stabilite între Spital şi furnizorii de stocare a copiilor de siguranţă în altă zonă trebuie să fie revizuite cel puţin anual.
4. Verificarea copiilor de siguranţă se va face după o procedură documentată şi revizuită periodic.
5. Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţiile 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 îşi schimbă locul de muncă.
7. Benzile sau mediile utilizate pentru stocarea copiilor de siguranţă trebuie să aibă un sistem de identificare care să conţină cel puţin următoarele date de identificare a informaţiei stocate:
- numele sistemului;
- data creării copiei;
- tipul de copie (completă, incrementală, etc.);
- clasificarea sensibilităţii (siguranţei/securităţii);
- informaţii de contact.

Anexa 10

Reguli de securizare a serverelor

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

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

Anexa 11

Reguli privind securitatea informaţiilor 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 reţele de tip wireless se poate face numai prin reţelele instalate de către administratorul de reţea; acestea vor utiliza tehnici de criptare pentru protejarea datelor transmise.
5. Toate accesările de la distanţă a Resurselor Informatice şi de Comunicaţii trebuie să se efectueze prin intermediul serviciului autorizat, conform *Regulilor de acces la reţeaua de comunicaţii (Anexa 3).*
6. Conectarea sistemelor de calcul care nu sunt proprietatea Spitalului se face numai cu aprobarea scrisă a managerului unităţii.

Anexa 12

Reguli pentru parolele de acces

1. Orice parolă ar trebui să fie complexă şi să aibă o lungime minimă de 8 caractere.
O parolă complexă este un şir de caractere compus din litere minuscule, majuscule, cifre şi simboluri (%$#&^* ...).
Criterii pentru stabilirea unei parole:
- nu este deloc recomandată folosirea simplă a datelor personale (ex: data naşterii, nume, prenume etc.) ca parole;
- folosiţi cifre şi simboluri uşor de asociat prin forma lor cu litere. De exemplu: a=@, B=8,E=3, i=1, I=!, O=0(zero), s=$. *Exemplu:* popescu1974 #p0p3$cu#!974
- faceţi asocieri dupa ceva ce vă place: o carte, titlul unei melodii, titlul unui film, personajele dintr-un film, etc. şi trasaţi-vă nişte reguli de formare a parolei pe care sa le folosiţi de fiecare dată când aveţi nevoie de o parolă nouă.

De exemplu: Prin asocierea iniţialelor (să hotărâm că le vom folosi ca litere minuscule) titlului filmului „Pulp fiction" cu primele două litere din numele şi prenumele personajelor *Vincent Vega* şi*Mia Wallace*, folosind cifre şi simboluri uşor de asociat cu litere (i=1, e=3, a=@), se poate obţine parola: pfV1V3M1W@. Nu trebuie să vă străduiţi foarte mult să ţineţi minte această parolă - care pare a fi complicată la prima vedere - pentru că o puteţi deduce logic de fiecare dată când aveţi nevoie de ea, important e sa ţineţi minte regulile după care aţi format-o.

2. Nu vă notaţi parolele pe hârtii.
3. Nu folosiţi aceeaşi parolă pentru mai multe conturi.
4. Dacă aveţi multe parole le puteţi scrie într-un fişier, însă criptaţi acel fişier şi asiguraţi-vă că nu-l veţi pierde. Evitaţi denumirea acelui fişier cu una explicită (*parolelemele.rar*).
5. Evitaţi să pastraţi parole în agende electronice, telefoane mobile – pot fi furate.
6. Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puţin o dată la 90 de zile.
7. Aveţi grijă la facilitatea browser-elor de reţinere a parolelor (*AutoFill, Remember password*) cu atât mai mult atunci când calculatorul pe care lucraţi e folosit de mai multe persoane.
8. Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor 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 şi o aprobare corespunzătoare.
2. Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor 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 şi 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 reţea trebuie să furnizeze o listă cu toţi utilizatorii (listă de conturi) pentru sistemele pe care le administrează.

Anexa 14

Reguli privind sistemul de mesagerie electronică

I. Activităţi strict interzise
- Trimiterea de mesaje cu caracter de intimidare sau hărţuire;
- 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 identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.

II. Activităţi interzise deoarece împiedică buna funcţionare a comunicaţiilor în reţea şi eficienţa sistemelor de mesagerie electronică:
- Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia;
- Trimiterea sau retrimiterea mesajelor ce pot conţine viruşi;
- Ignorarea cererii administratorului reţelei de a elibera spaţiile de pe server pe care le ocupă.

III. Alte menţiuni
- Toate informaţiile şi datele confidenţiale ale Spitalului, transmise către alte reţele externe, trebuie să fie criptate.

- Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea resurselor informatice şi de comunicaţii ale Spitalului pot fi oricând înregistrate şi analizate.
- Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că îşi spun opinia sau dau declaraţii în numele Spitalului, 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 Spitalul.
Un exemplu de declaraţie simplă este: "părerile exprimate sunt personale, şi nu ale Spitalului ... ".
- Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informaţii confidenţiale sau nesigure, ce privesc Spitalul, folosind dispozitive de comunicaţii mobile care nu sunt autorizate de Spital. *Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt*: telefoane mobile, asistenţi digitali personali, pagere ce permit trimiterea/primirea de informaţii.
- Reţeaua Spitalului se declară a fi un mediu de lucru şi comunicare academic, deschis şi civilizat. Utilizatorii sunt invitati să se trateze reciproc în mod politicos şi cordial. Spiritul Internet presupune dialoguri într-un stil caracterizat prin decenţă, amabilitate şi bunăvoinţă. Partenerii nostrii din Internet se aşteaptă să găsească în Spital un mediu academic atunci când solicită informaţii despre noi, motiv pentru care, utilizatorii vor lua măsuri pentru a se autoidentifica corect atât pe serverul Spitalului, cât şi în corespondenţa electronică pe care o trimit.

Anexa 15

Reguli de detectare a virusilor

1.Toate statiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Spitalului trebuie să utilizeze programe antivirus aprobate de către administratorul de sistem .
2. Programele antivirus nu trebuie sa poata fi dezactivate de catre utilizatori.Acestea trebuie sa fie tot timpul active
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 sa fie zilnica**5.** Orice server de fişiere conectat la reţeaua instituţiei trebuie să utilizeze un program antivirus aprobat, în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.
5. 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 de utilizare a acestui program.
6. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie sa fie raportat imediat administratorului de sistem in mod automat.

Anexa 16

Reguli de relaţii cu terţii

1. În toate convenţiile şi contractele încheiate cu Furnizorii trebuie specificate:
- informaţiile din cadrul Spitalului, 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 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 informaţie din sistemul RIC al Spitalului obţinută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.
4. Toate echipamentele de întreţinere ale Furnizorului aflate în reţeaua internă a Spitalului şi care se pot conecta în exterior prin intermediul reţelei, precum şi toate conturile de utilizator create temporar pentru Furnizor şi necesare pentru acces la RIC ale Spitalului vor fi scoase din uz la încheierea relaţiilor contractuale.

5. Accesul Furnizorului trebuie să fie identificat în mod unic, iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu *Regulile privind parolele de acces* şi *Regulile de acces administrativ*.
6. Activităţile principale ale Furnizorului trebuie să fie documentate de acesta şi puse la dispoziţia 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 şi de livrare.
7. 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 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 informaţiile ce aparţin Spitalului şi va oferi certificare în scris privind predarea sau distrugerea informaţiilor 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 legitimaţiile, echipamentele şi stocurile Spitalului. Echipamentele şi/sau stocurile care urmează a fi reţinute de către Furnizor trebuiesc documentate şi autorizate de Conducerea Spitalului .
10. Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către Spital trebuie să fie inventariate corespunzător si să posede drepturi de utilizare atestate prin Licenţe.

Anexa 17

Reguli pentru modificări şi modernizări ale RIC

Orice modificare asupra unei componente ale RIC din cadrul Spitalului (cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii) trebuie să respecte regulile de mai jos:
1. 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) trebuie să fie anunţate şi aprobate în scris.
2. Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RIC vor fi documentate şi aprobate de către conducere. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RIC.
3. Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducere.
4. Modificările planificate trebuie anunţate cu cel putin 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 instituţiei 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 întreţinută o bază de date care să cuprindă toate modificările. Aceasta trebuie să conţină cel puţin următoarele informaţii:
- data la care s-a făcut cererea pentru modificare şi data la care s-a făcut modificarea;
- informaţii de contact pentru utilizator;
- natura modificării;
- indicarea succesului sau nereuşitei modificării.

Anexa 18

Procedură pentru alocarea unei adrese de email. Cerere tip

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

1. Toti angajaţii au dreptul de a deţine o adresă de email pe serverul Spitalului.

2. Se recomandă ca adresa de email să fie de forma: *nume@spitalpsihiatrieborsa.ro* sau *prenume.nume@spitalpsihiatrieborsa.ro* sau *inume@spitalpsihiatrieborsa.ro* (unde i reprezintă iniţiala prenumelui)

3. Cererile de obţinere a unui cont de email pe serverul Spitalului este prezentata in modelul alăturat, se completează de către solicitant și se depune spre aprobare managerului.

4. Pentru verificarea căsuţei poştale este pusă la dispoziţie o interfaţă web la adresa *http://webmail.spitalpsihiatrieborsa.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 aprobaţi deschiderea unui cont de email pe domeniul *spitalpsihiatrieborsa.ro*.
Numele de utilizator propus este: _____
(*se recomandă folosirea numelui, eventual precedat de prenume sau de iniţiala prenumelui*).

Solicit ca mesajele primite pe acest cont de email să fie redirecţionate automat :
Da, către adresa : _____
şi doresc să păstrez mesajele şi în contul deschis pe *spitalpsihiatrieborsa.ro*: Da Nu
Nu

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

Data:_____ Semnătura_____

Anexa 19

Procedură pentru conectarea la reţea. Cerere tip

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

1. Toate cadrele medicale și angajații care aparţin personalului administrativ pot solicita conectarea la reţeaua administrativă a Spitalului.
2. Cererea de conectare la reţeaua administrativă a Spitalului este prezentată în modelul alăturat, se completează de beneficiar şi se depune spre aprobare managerului.

Observaţie:
Adresa fizică (*MAC address*) a calculatorului/laptop-ului pentru care se doreşte conectarea la reţea se afla prin succesiunea de comenzi:
Start → Run (Search) → cmd → ipconfig –all

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

Orice alte precizări necesare pentru conectarea la reţeaua 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 REŢEA

Subsemnatul/a,_____
angajat al Spitalului de Boli Psihice Cronice Borșa în funcția de _____,
Compartimentul/Secția_____, vă rog să-mi aprobaţi conectarea la reţeaua 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 şi securitatea Resurselor Informatice şi de Comunicaţii* din cadrul Spitalului de Boli Psihice Cronice Borșa şi să-l consult periodic pentru a fi la curent cu eventualele modificări survenite.

De asemenea, menţionez că am luat la cunoştinţă faptul că nerespectarea acestuia poate duce la luarea unor măsuri de restricţie a accesului meu la facilităţile reţelei de comunicaţii digitale a Spitalului de Boli Psihice Cronice Borșa.

Data:_____ Semnătura_____

Anexa 20

Proces verbal de constatare

PROCES VERBAL DE CONSTATARE
Întocmit astăzi, ___ /___ /20.., între:

- _____administrator de sistem
şi
- beneficiarul, _____, de la Departamentul _____
(telefon: _____, email: _____)
privind constatarea defecţiunilor echipamentului de mai jos.

Echipament:

_____

Este în garanţie : da.....nu.....
Defect reclamat:

Defect constatat:

Recomandări:

Încheiat în două exemplare cu următoarea destinaţie: un exemplar rămâne în evidenţa administratorului de sistem, iar pe cel de-al doilea îl primeşte beneficiarul.

Anexa 21

Exemple de activităţi interzise

Activităţi comerciale neautorizate:
- Trafic masiv de informaţii sau trafic de informaţii cu caracter frivol, obscen şi pornografic;
- Folosirea unor drepturi de acces la resurse pentru care nu sunt autorizaţi;
- Ştergerea sau alterarea datelor altor utilizatori;
- Tentativele de descoperire şi de folosire a parolelor altor utilizatori;
- Crearea sau folosirea de instrumente soft destinate spargerii sistemelor de securitate ale calculatoarelor;
- Provocarea deliberată de defectiuni hardware şi software;
- Perturbarea traficului reţelei 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 aplicaţii de tip virus, troieni, viermi, spyware sau altele;
- Folosirea de aplicaţii de tip key-logere;
- Modificarea adresei MAC a plăcii de reţea;
- Setările pentru IP şi DNS altfel decât cu "Obtain an IP/DNS address automatically";
- Utilizarea de programe pentru scanarea reţelei, exploit-uri;
- Realizarea de tunele;
- Transmiterea de mesaje cu caracter comercial;
- Publicitatea cu caracter comercial;
- Folosirea de software fără licenţă pe calculatoarele din Spital sau conectate la reteaua Spitalului.

ANALIZA RISCURILOR SISTEMULUI IT

DIN CADRUL SPITALULUI DE BOLI PSHICE CRONICE BORŞA

Analiza riscului constituie un compartiment al abordării sistemice a luării deciziilor, realizării procedurilor şi acţiunilor practice în procesul de soluţionare a problemelor de avertizare (preîntâmpinare), ori de reducere a pericolului întreruperii funcţionării sistemului informaţional al Spitalului.

Esenţa gestiunii riscului se reduce la colectarea şi analiza informaţiilor privind funcţionarea sistemului informaţional în ansamblu şi a fiecărei componente a lui, la analiza riscului (pericolului) şi controlului funcţionării sistemului de securitate informaţională.

Procedura analizei riscului este parte componentă a planului de securitatea IT implementat la nivelul Spitalului, analizei economice în baza criteriilor "valoare–securitate-profit"; asigurării şi a altor categorii de analize şi estimare a situaţiei securităţii sistemului informaţional.

Sarcina de bază a analizei riscului constă în oferirea informaţiilor obiective privind funcţionarea sistemului informaţional 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 frecvenţei)
3. Care pot fi consecinţele? (analiza consecinţelor)

De asemenea analiza în cauză poate fi considerată drept remediu eficace, în cadrul şi graţie căreia sunt determinate modalităţile de abordare a depistării pericolelor şi riscurilor, se întreprind acţiuni de formulare a deciziilor obiective referitor la nivelul riscului posibil, la stabilirea exigenţelor şi recomandărilor privind reglarea securităţii examinate.

Sunt posibile mai multe variante ale strategiei securităţii funcţionării sistemului informaţional (S.I.) în condiţii de luare a deciziilor în situaţii de incertitudine, dar de bază sunt următoarele trei:

1. Prima variantă constă în ***evitarea riscului***. Ea se reduce la refuz de acţiuni ce ar conduce la anumit risc, precum şi din temeri de consecinţe defavorabile şi din motiv că cele întreprinse în principiu nu pot avea loc în procesul funcţionării S.I. De exemplu, chiar şi în S.I. local închis efectiv poate exista riscul pierderilor de informaţii provocate de intervenţii ale utilizatorilor atât la nivel fizic, cât şi logic şi semantic. Pe lângă aceasta, e necesar de ţinut cont de faptul, că S.I. încorporează o mulţime considerabilă de componente, care dispun de colecţii de diverşi parametri tehnici (timpul prelucrării refuzului, probabilitatea refuzului ş.a.).
2. A doua variantă este ***acceptarea riscului***. Această strategie este legată de faptul că administratorul, în mod conştient, recurge la risc până atunci când consecinţele riscurilor ce s-au produs nu vor conduce la pierderi irecuperabile. Varianta examinată nu poate fi considerată optimală, aşa acum nu exclude consecinţe fatale.
3. A treia variantă a strategiei securităţii S.I. se reduce la **gestiunea riscului**. Ea constă în determinarea şi estimarea, precum şi elaborarea acţiunilor (măsurilor) minimizării riscului. De menţionat că gestiunea riscurilor este un domeniu interdisciplinar specific, care solicită cunoştinţe fundamentale referitoare la teoria sistemelor complexe (compuse), teoria protecţiei informaţiei ş.a.

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

- ***diminuarea riscului*** prin aplicarea remediilor simple şi accesibile, cum ar fi de exemplu, organizarea raţională a gestiunii parolelor utilizatorilor, care de cele mai multe ori reduce pericolul accesului nesancţionat;
- ***evaziune de la risc*** prin intermediul acţiunilor de ordin organizatoric;
- ***schimbarea caracterului riscului*** pe contul funcţiei asigurării în cazurile apariţiei situaţiilor imprevizibile;
- ***acceptarea riscului*** contând pe strategia gestiunii lui.

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

Actualmente sunt cunoscute următoarele varietăţi de riscuri şi indicatori ce-i caracterizează:

- ***risc individual*** – caracterizat în baza unui indicator cum ar fi frecvenţa defectării unei componente a sistemului (de exemplu: calculatorul, sistemul de operare, aplicaţia programată, baza de date ş.a.) provocată de influenţa 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 informaţionale ş.a.);
- ***risc potenţial*** – caracterizat prin distribuirea spaţială a frecvenţei influenţei negative de anumit nivel asupra sistemului;
- ***risc social*** - caracterizat de frecvenţa evenimentelor negative, în urma cărora au suferit utilizatorii sistemului.

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

- evidenţierea 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 paşi efectuaţi în următoarea succesiune:

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

Pasul 2 - Formarea listei ameninţărilor posibile şi probabile. Drept ameninţare se consideră orice acţiune, care ar provoca deschideri neautorizate, distrugeri, modificări şi refuz de deservire. Prin urmare, în cadrul acestei etape are loc identificarea mulţimii de ameninţări, cu concretizarea cât mai satisfăcătoare a probabilităţii (frecvenţei) lor şi a pierderilor aşteptate.

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

Pasul 4 - Determinarea remediilor posibile de opunere şi verificarea ameninţărilor, evidenţierea remediilor, costurilor şi eficienţei lor.

Pasul 5 - Calcularea şi determinarea rezultatelor financiare, obţinute de la realizarea fiecărui remediu de opunere ameninţărilor, prin contrapunerea cheltuielilor şi profitului de la efectuarea lor.

Pasul 6 - Determinarea şi formularea recomandărilor privind selectarea remediilor de opunere şi de verificare a ameninţărilor. În cazul selecţiei metodelor de opunere şi verificare a acestor ameninţări e necesar de ţinut cont de tipul S.I., caracterul ameninţărilor (posibile şi potenţiale), scopurile analizei, criteriile riscului admisibil, dispunerea de recurse necesare pentru efectuarea analizei, de informaţii respective, de experienţa şi calificarea executorilor ş.a.

După **scopurile urmărite** ameninţările pot fi sistematizate în următoarele categorii:

- violarea integrităţii informaţiilor,;
- violarea accesibilităţii informaţiilor ori capacităţii de funcţionare a sistemului ;
- violarea confidenţialităţii informaţiilor; informaţiile păstrate şi prelucrate de sistem;
- violarea valorii şi semnificaţiei juridice a informaţiilor.