Regulamentul privind politicile de securitate IT

Anexa 1

REGULI DE UTILIZARE
a Resurselor Informatice şi de Comunicaţii

A. Utilizarea permanentă a Resurselor Informatice şi de Comunicaţii

1. Utilizarea Resurselor Informatice şi de Comunicaţii se face numai în interes de serviciu.

2. Utilizatorii trebuie să anunţe Serviciul de Informatica atât despre orice problemă/breşă în sistemul de securitate din cadrul Spitalului Municipal "Dimitrie Castroian" Husi, 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 în cadrul Resurselor Informatice şi de Comunicaţii Spitalului Municipal "Dimitrie Castroian" Husi.

4. Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din Resursele Informatice şi de Comunicaţii 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 aprobarea Serviciului de Informatica.

8. Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane; să degradeze performanţele sistemelor ce alcătuiesc Resursele Informatice şi de Comunicaţii; să împiedice accesul unui utilizator autorizat la Resursele Informatice şi de Comunicaţii; 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 Resursele Informatice şi de Comunicaţii. De exemplu, utilizatorii SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis .

10. Resursele Informatice şi de Comunicaţii ale SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI nu trebuie să fie folosite pentru beneficiul personal.

11. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI le poate considera ofensive sau indecente.

12. Accesul la reţeaua Internet prin intermediul Resursele Informatice şi de Comunicaţii 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 Resursele Informatice şi de Comunicaţii SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI.

14. Utilizatorii care au acces la Resursele Informatice şi de Comunicaţii SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI 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 Resursele Informatice şi de Comunicaţii Spitalului Municipal "Dimitrie Castroian" Husi.

16. Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI folosind Resursele Informatice şi de Comunicaţii.

17. Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni ilegale împotriva SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI.

18. Toate mesajele, fişierele şi documentele localizate în cadrul Resurselor Informatice şi de Comunicaţii sunt proprietatea SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI 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 Resurselor Informatice şi de Comunicaţii. În aceste situaţii se aplică următoarele restricţii:

- utilizarea personală ocazională a serviciilor de poştă electronică, acces Internet, 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
de acces la reţeaua de comunicaţii

1. Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către Serviciul Informatica.

2. Departamentele şi Sectiile trebuie să ceara in scris, conectarea dispozitivelor de calcul la RIC ale SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI. 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 Serviciul Informatica. Conectarea se face numai cu avizul Serviciului informatica .

3. Conectarea sistemelor de calcul care nu sunt proprietatea SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI se face numai cu aprobarea în scris a Serviciul Informatica la recomandarea Departamentelor sau a Sectiilor.

4. Accesul de la distanţă la reţeaua SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI şi folosind protocoale aprobate de către Serviciul Informatica.

5. Utilizatorii RI din interiorul SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI nu se pot conecta la altă reţea.

6. Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în niciun fel, pe nicio cale. Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Sectiilor şi a Departamentelor de către Serviciul Informatica.

7. Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea Serviciul Informatica.

8. Sistemele computerizate din afara SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI.

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 MUNICIPAL "DIMITRIE CASTROIAN" HUSI nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI.

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 Serviciul Informatica.

12. Serviciile de interconectare a reţelei SPITALULUI MUNICIPAL "DIMITRIE CASTROIAN" HUSI cu alte reţele sunt realizate exclusiv de către Serviciul Informatica.

13. Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Serviciului de Informatica. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către Serviciul Informatica.

14. Accesul tertilor la RI sa va face numai cu notificare scrisa sau prin email si numai cu acordul Serviciului Informatic, folosind o solutiie de conectare agreata de Serviciul de Informatica. Notificarea trebuie sa contina :

- Numar de identificare / Data interventiei / Scopul interventiei / Durata interventiei /Date de contact ale persoanei care face interventia

- In vederea monitorizarii comunicarii, toate mesajele utilizate vor fi prefixate in sectiunea “Subiect” cu numarul de identificare.

- Conturile de acces vor avea drepturi specifice si se vor acorda numai pe durata interventiei

Anexa 3

REGULI
de acces administrativ

1. Departamentele şi Sectiile trebuie să prezinte la Serviciul de Informatică o listă cu informaţii de contact în plan administrativ pentru toate sistemele conectate la reţeaua de comunicaţii a Spitalului. Această listă trebuie refăcută şi prezentată la Serviciul de Informatică de fiecare dată când apar modificări de orice natură.

2. Utilizatorii trebuie să cunoască şi să accepte toate regulamentele privind securitatea RI 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 Departament sau Sectie 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 Serviciul de informatica şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă din cadrul Departamentului, Sectiei sau a Spitalului, sau în cazul unei modificări a listei de personal ale terţilor (furnizor desemnat) în contractele cu Spitalul.

Anexa 4

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 Serviciul de Informatica care este responsabilă 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 Serviciul de Informatica sau de către un furnizor avizat explicit de către Serviciul de Informatica. Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor Serviciul de Informatica.

3. Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai cu aprobarea Serviciului de Informatica.

4. Infrastructura de comunicaţii de date a Spitalului suportă un set definit de protocoale de reţea. Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către Serviciul de Informatica.

5. Adresele de reţea sunt alocate dinamic sau static numai de către Direcţia de Informatică.

6. Toate conectările în reţeaua de comunicaţii a Spitalului sunt responsabilitatea Serviciului de Informatică, conectarea se va face numai în baza unei cereri standard aprobată de către Departament sau Sectie. Formularele vor fi puse la dispoziţie prin intermediul site-ului web al Serviciului de Informatica.

7. Toate conectările dintre reţeaua de comunicaţii a Spitalului şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a Serviciului de Informatica.

8. Echipamentele de protecţie a reţelei de comunicaţie a Spitalului (firewall) se vor instala de către Serviciul de Informatica.

9. Utilizarea sistemelor de protecţie (firewall) din Departamente şi Sectii nu este permisă fără autorizaţie scrisă din partea Serviciului de Informatica. Această restricţie se aplică şi în cazul în care se folosesc adrese private de reţea.

10. Utilizatorii nu au dreptul să extindă sau să retransmită în niciun fel serviciile reţelei (este interzisă instalarea unui modem, router, switch, hub sau punct de acces la reţeaua Spitalului) fără aprobare din partea Serviciului de Informatica.

11. Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau programe care furnizează servicii de reţea fără aprobarea Serviciului de Informatica.

12. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

Anexa 5

REGULI
de tratare a incidentelor de securitate

1. În cazul incidentelor de securitate din cadrul Spitalului Municipal "Dimitrie Castroian" Husi, membrii Serviciului Informatică 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. Serviciul de Informatică este responsabilă cu înştiinţarea şi coordonarea pentru tratarea incidentului.

4. Serviciul de Informatică este responsabil cu 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. Serviciul de Informatică va stabili conţinutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informaţii.

7. Serviciul de Informatică trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.

8. Serviciul de Informatică este responsabil cu documentarea anchetei privind incidentul.

9. Serviciul de Informatică este responsabil de coordonarea activităţilor de comunicare cu terţi pentru rezolvarea incidentului.

10. În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare Serviciul de Informatică va recomanda sancţiuni disciplinare.

Anexa 6

REGULI
de monitorizare a Resurselor Informatice şi de Comunicaţii

Monitorizarea Resurselor Informatice (RI) şi de 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 RI, 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.

Serviciul de informatica va efectua, în mod regulat (cel puţin o dată pe an), 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 routere/modem-uri neautorizate;
- Licenţelor pentru sistemele de operare şi programele instalate.

Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către Serviciul de informatica în scopul efectuării de investigaţii.

Anexa 7

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) periodic de către administratorul de sistem.

5. Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip firewall sau dispozitive de control al accesului.

6. Înregistrările de verificare pentru serverele şi host-urile din reţeaua internă trebuie revizuite periodic.

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 de utilizatori imediat către Serviciul de Informatica.

10. Utilizatorii sunt obligaţi să raporteze Serviciul de Informatică orice anomalii în performanţa sistemelor utilizate sau orice semne ale unor posibile infracţiuni.

Anexa 8

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 de catre utilizator utilizând tehnici aprobate Serv. Informatica.

4. Transmiterea datelor prin reţele de tip wireless se poate face numai prin reţelele instalate de către Serviciul de Informatică, 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 2).

6. Conectarea sistemelor de calcul care nu sunt proprietatea Spitalului se face numai cu aprobarea scrisă a Serviciului de Informatică , la recomandarea Departamentelor sau Sectiilor.

Anexa 9

REGULI
privind parolele de acces

1. Orice parolă ar trebui să fie complexă
O parolă complexă este un şir de caractere compus din litere minuscule, majuscule, cifre şi simboluri (%$#&^* …).

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 180 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 10

REGULI
de administrare a conturilor de email

1. Fiecare cont de email trebuie sa fie creat pe domeniul http://spitalulmunicipalhusi.ro/
2. Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces. asociat.
3. Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont
4. Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Regulile privind Parolele de Acces (Anexa 9).
5. Utilizatorilor **nu le este permis** să păstreze în directoarele proprii de pe server (Inbox, Sent, Trash) **mesaje mai vechi de 14 zile calendaristice**. În caz contrar, **după 21 de zile calendaristice** mesajele vor fi **şterse automat**. Excepţie de la această regulă fac persoanele care au funcţii de conducere, precum şi cele din secretariate.

6. La cererea conducerii autorizate din Spital, Serviciul de Informatică trebuie să furnizeze o listă cu toţi utilizatorii (listă de conturi) pentru sistemele pe care le administrează.

Anexa 11

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
- 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 mesajelor de dimensiuni foarte mari;
- Trimiterea sau retrimiterea mesajelor ce pot conţine viruşi.
- Ignorarea cererii administratorului reţelei de a elibera spaţiile de pe server pe care le ocupă. Conform Regulilor de administrare a conturilor de email, toţi utilizatorii (cu excepţia persoanelor care au funcţii de conducere şi a celor din secretariate) se obligă să menţină în directoarele proprii de pe serverul de mail numai mesajele din cel mult ultimele 14 zile.

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 Spitala. 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.

Anexa 12

REGULI
privind detectarea viruşilor

1. Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Spitalului, trebuie să utilizeze programe antivirus aprobate de către Serviciul de Informatică.

2. Programele antivirus nu trebuie dezactivate.

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

4. Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

5. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat Serviciului de Informatică.

Anexa 13

REGULI
pentru modificări şi modernizări
ale Resurselor Informatice şi de Comunicaţii

Orice modificare asupra unei componente a Resurselor Informatice (RI) 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 de către Departamentul sau Sectia care administrează resursele afectate.

2. Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RI vor fi documentate şi aprobate de către Serviciul de Informatică . Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RI.

3. Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducerea Departamentului sau Sectiei si avizate de Serviciul de Informatica.

4. Orice cerere de modificare planificată trebuie să obţină o aprobare formală din partea Departamentului sau Sectiei care administrează resursele supuse modificărilor.

5. Modificările planificate trebuie anunţate cu cel putin 48 ore înainte de a fi executate.

6. 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.

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

8. 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 14

PROCEDURĂ PENTRU
ALOCAREA UNEI ADRESE DE EMAIL

Se adresează cadrelor medicale, personalului de administraţie din Spital care doresc deschiderea unui cont de email pe domeniul http://spitalulmunicipalhusi.ro/

1. Toate cadrele medicale, toţi angajaţii care aparţin personalului administrativ, tehnic au dreptul de a deţine o adresă de email in cadrul Spitalului.

2. Se recomandă ca adresa de email să fie de forma:
nume.prenume@spitalulmunicipalhusi.ro

3. Cererile de obţinere a unui cont de email pe Spital se downloadează de pe http://spitalulmunicipalhusi.ro şi se depun la Serviciul Informatica.

4. Pentru verificarea căsuţei poştale este pusă la dispoziţie o interfaţă web la adresa http://spitalulmunicipalhusi.ro/webmail
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). Motivul principal este acela că, pentru a se asigura o funcţionare optimă a serviciului de email, utilizatorilor nu le este permis să păstreze în directoarele proprii de pe server mesaje mai vechi de 14 zile.

CERERE DE DESCHIDERE A UNUI CONT DE EMAIL

Subsemnatul/a,_____ angajat al Spitalului Municipal "Dimitrie Castroian" Husi in functia de _____, departament/sectie/serviciu/birou _____telefon _____
vă rog să-mi aprobaţi deschiderea unui cont de email pe domeniul http://spitalulmunicipalhusi.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 http://spitalulmunicipalhusi.ro/:
Nu ☐

Prin semnarea acestui document mă angajez să respect Regulamentul privind utilizarea şi securitatea Resurselor Informatice din cadrul reţelei http://spitalulmunicipalhusi.ro/ a Spitalului Municipal "Dimitrie Castroian" Husi

Anexa 15

PROCEDURĂ PENTRU CONECTAREA LA REŢEA

Se adresează angajatilor Spitalului Municipal "Dimitrie Castroian" Husi care doresc să se conecteze la reţeaua Internet a Spitalului.

1. Toti angajatii care au in gestiune un calculator pot solicita conectarea la reţeaua Internet a Spitalului daca activitatea pe care o desfasoara necesita conectarea la internet si are aprobare de la Departamentul sau Sectia de care apartin .

CERERE DE CONECTARE LA REŢEA

Subsemnatul/a,_ angajat al Spitalului Spitalului Municipal "Dimitrie Castroian" Husi in functia de , departament/sectie/serviciu/birou vă rog să-mi aprobaţi conectarea la reţeaua internet a Spitalului Municipal "Dimitrie Castroian" Husi 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 din cadrul reţelei Spitalului Municipal "Dimitrie Castroian" Husi (disponibil pe http://spitalulmunicipalhusi.ro/) 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 Municipal "Dimitrie Castroian" Husi.

Data:

Semnătura_

Aprobat Manager,
Dr. Roraru Lucia

Anexa 16

PROCES VERBAL DE INTERVENŢIE IT

Se completează de către utilizator. Toate rubricile sunt obligatorii.

Echipament: ..... Locaţie: .....
Utilizator: ..... Telefon: .....
Defect semnalat:.....
.....
Doresc păstrarea datelor de pe hard disc: DA / NU
IMPORTANT! În cadrul departamentului IT se încearcă păstrarea aplicaţiilor şi a datelor de pe hard disc, dar nu vă putem asigura că acestea nu au fost deja pierdute (hard disc defect) sau că nu vor fi pierdute în timpul intervenţiei (devirusare, reinstalare). Vă rugăm să acordaţi atenţie faptului că responsabilitatea pentru o salvare completă a datelor pe un suport extern (Memorie USB, CD, DVD) vă revine în totalitate dumneavoastră ca utilizator al calculatorului.
Data predării pentru reparaţie: ..... Predat de: .....
.....

Preluat de: .....
.....
Defect constatat: .....
.....
Operaţii efectuate: .....
.....
.....
Componente folosite: .....
.....
.....
Recomandări: .....
.....
.....
Executat de: ..... Data: .....
Data predării: .....
Predat de: .....
.....
Primit de: .....

Anexa 17

EXEMPLE
de activităţi interzise în reţeaua Spitalului Municipal "Dimitrie Castroian" Husi

- 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;
- Instalarea de programe altele decat cele aprobate de Serv . Informatica
- 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 Municipal "Dimitrie Castroian" Husi
- Generarea de trafic care nu este specific activitatilor spitalului(torente,streeming,etc)
- Transferuri de materiale care contravin legilor drepturilor de autor (software pirat, filme, muzică etc.);
- Generarea de spam;
- Jocuri online,filme online,videostreeming in timpul programului de lucru;
- 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 cele setate de Serv Informatica;
- Utilizarea de programe pentru scanarea reţelei, exploit-uri;
- Realizarea de tunele, sau alte aplicatii care sa ocoleasca sistemul de securitate (firewall,etc)
- Transmiterea de mesaje cu caracter comercial;
- Publicitatea cu caracter comercial;