UNIVERSITATEA DE ŞTIINŢE AGRICOLE ŞI MEDICINĂ VETERINARĂ CLUJ-NAPOCA
Calea Mănăştur 3-5, 400372, Cluj-Napoca
Tel: 0264-596.384, Fax: 0264-593.792
www.usamvcluj.ro

Planul de Securitate a sistemului Resurselor Informatice şi de Comunicaţii

Introducere

Regulamentele de Utilizare a Resurselor Informatice şi de Comunicaţii sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în Universitatea de Ştiinţe Agricole şi Medicină Veterinară din Cluj-Napoca.

Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea acestea au ca scop protejarea imaginii Universităţii şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţii.

Scop

În acord cu legislaţia în vigoare în România, Regulamentele de ordine interioară ale Universităţii de Ştiinţe Agricole şi Medicină Veterinară din Cluj-Napoca, Resursele Informatice şi de Comunicaţii sunt valori ale Universităţii care trebuie exploatate şi administrate ca resurse publice în proprietatea statului român. Scopul acestor regulamente este acela de a asigura:

- Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţii în vederea sprijinirii procesului educaţional şi a cercetării ştiinţifice.
- Protejarea imaginii Universităţii.
- Protejarea investiţiilor Universităţii pentru dezvoltarea sistemului informatic şi de comunicaţii propriu.
- Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate folosind Resursele Informatice şi de Comunicaţii ale utilizatorilor autorizaţi: cadre didactice, personal administrativ, studenţi, colaboratori etc.
- Educarea utilizatorilor resurselor informatice şi de comunicaţii în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora.
- Compatibilitate cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

Audienţă

Regulamentele de utilizare a resurselor informatice şi de comunicaţii ale Universităţii de Ştiinţe Agricole şi Medicină Veterinară din Cluj-Napoca se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acestea.

Proceduri de elaborare, modificare şi aprobare a Regulamentelor

- Regulamentele de utilizare a Resurselor Informatice şi de Comunicaţii ale Universităţii se elaborează pentru fiecare activitate specifică domeniului şi trebuie concepute în aşa fel încât fiecare Regulament să poată fi folosit cvasi-independent de celelalte.
- Regulamentele vor fi elaborate de către Centrul de Informatizare si Comunicatii şi vor fi propuse pentru aprobare conducerii Universităţii de Ştiinţe Agricole şi Medicină Veterinară din Cluj-Napoca.
- Prevederile Politicii de Securitate aprobate vor fi incluse în contractul de muncă, contractul cu studenţii şi toate contractele cu terţi (dacă activitatea acestora are legătură cu sistemul Informatic şi de Comunicaţii al Universităţii).
- Fiecare Regulament va conţine informaţii de identificare proprii şi se va specifica data la care acesta a fost aprobat şi data de la care acesta este aplicabil.
- Regulamentele de utilizare a sistemului Resurselor Informatice şi de Comunicaţii vor fi disponibile în format electronic pe site-ul universității www.usamvcluj.ro.
- Modificarea prevederilor unui Regulament se face cu aprobarea conducerii Universităţii. Fiecare modificare va include modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune este aplicabilă.
- Prezentul document va fi conţine o listă a tuturor regulamentelor aplicabile în sistemul Resurselor Informatice şi de Comunicaţii.

Proceduri şi Regulamente Specifice:

1. Utilizarea Permanentă a Resurselor Informatice şi de Comunicaţii

- Utilizatorii trebuie să anunţe CIC în cazul în care se observă orice problemă/breşă în sistemul de securitate a RIC din cadrul Universităţii cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.
- Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip în cadrul sistemului RIC al Universităţii.
- Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din RIC pentru care nu au autorizaţie sau consimţământ explicit.
- 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.
- Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).
- Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane; să degradeze performanţele RIC; să împiedice accesul unui utilizator autorizat la RIC; să obţină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente.
- Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii RIC. De exemplu, utilizatorii nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente.
- RIC ale Universităţii nu trebuie folosite pentru beneficiul personal.
- Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Universitatea le poate considera ofensive, indecente sau obscene (altele decât cele în curs de cercetare academică unde acest aspect al cercetării are aprobarea explicită a conducerii Universităţii).
- 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. Angajaţii nu trebuie să permită membrilor familiei sau altor persoane accesul la RIC ale Universităţii.
- Utilizatorii care au acces la sistemul RIC al Universităţii au obligaţia de a purta acte şi sau legitimaţii care să ateste calitatea de utilizator autorizat în spaţiile Universităţii. .
- Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor Universităţii folosind RIC.

2. Utilizarea Ocazională

- 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 utilizatorii 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 Universitate.
- Utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaţilor.
- Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Universităţii sau prejudicierea, indiferent de formă, a intereselor Universităţii.

3. Regulament privind Confidenţialitatea Serviciilor Informatice şi de Comunicaţii

- Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Universităţii, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea CIC).
- Un mare număr de utilizatori (inclusiv studenţi), pot accesa informaţii din exteriorul sistemului de comunicaţii al Universităţii. În aceste condiţii este obligatorie păstrarea confidenţialităţii informaţiilor transmise din exteriorul RIC şi a informaţiilor obţinute din interior.
- Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Universităţii pentru care nu au autorizaţie sau consimţământ explicit.
- Nici un utilizator al sistemului RIC al Universităţii nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului RIC. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu Universitatea.
- 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 Universităţii se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

4. Regulament de Acces Administrativ

- Departamentele şi Facultăţile Universităţii trebuie să prezinte la CIC o listă cu informaţii de contact în plan administrativ pentru toate sistemele conectate la reţeaua de comunicaţii a Universităţii. Această listă trebuie refăcută şi prezentată la CIC de fiecare dată când apar modificări de orice natură.
- Utilizatorii trebuie să cunoască şi să accepte toate regulamentele privind securitatea RIC înainte de a li se permite accesul la un cont.

- 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 Facultate şi vor fi incluse în fişa postului.
- Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi şi trebuie să facă investigaţii numai sub îndrumarea CIC.
- 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.
- Accesul administrativ trebuie să se conformeze Regulamentului de utilizare a Parolelor.
- Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al CIC şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă din cadrul Departamentului, Facultăţii sau a Universităţii, sau în cazul unei modificări a listei de personal ale terţilor (furnizor desemnat) în contractele cu Universitatea.
- Trebuie să existe o procedură prin care o altă persoană, în afară de administrator, să poată avea acces la contul administratorului în caz de forţa majoră. Această procedură va fi elaborată de către CIC pentru fiecare Facultate şi Departament.
- 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.

5. Regulament privind Accesul Fizic la RIC

- Toate sistemele de securitate fizică (de exemplu coduri de acces în clădire şi coduri de acces pentru prevenirea incendiilor etc.) a RIC trebuie să fie instalate în conformitate cu regulamentele Universităţii.
- Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat şi monitorizat.
- Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.
- 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.
- Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.
- Acordarea drepturilor de acces (folosind card-uri, chei, parole etc.) se face în scris de către CIC sau, după caz, Departamentul sau Facultatea care deţine încăperea şi resursele.
- Nu este permis transferul dreptului de acces indiferent de motiv.
- Cardurile şi/sau cheile de acces care nu mai sunt folosite trebuie predate Departamentului sau Facultăţii care le-a eliberat.

- Pierderea sau furtul cardurilor şi/sau cheilor de acces trebuie raportate imediat Departamentului sau Facultăţii care le-a eliberat.
- Cardurile şi/sau cheile nu trebuie să aibă informaţii de identificare, altele decât informaţia de contact necesară pentru returnare.
- Accesul vizitatorilor în spaţiile protejate trebuie documentat pentru fiecare începere şi, în cazul în care este permis, se va delega un însoţitor. Vizitatorii trebuie să fie însoţiţi în zonele cu acces restricţionat.
- Fiecare Departament şi Facultate va ţine o evidenţă a tuturor cardurilor şi/sau cheilor de acces emise, retrase, pierdute sau furate.
- Pentru fiecare spaţiu în care sunt instalate RIC se va păstra o evidenţă a accesului pentru verificări de rutină în situaţii critice.
- Fiecare Departament şi/sau Facultate trebuie să verifice periodic drepturile de acces pe bază de card şi/sau cheie şi să anuleze aceste drepturi pentru persoanele care pierd dreptul de acces.
- Fiecare Departament şi/sau Facultate trebuie să anuleze drepturile de acces ale cardurilor şi/sau cheilor utilizatorilor care îşi schimbă locul de muncă din Universitate sau nu au relaţii contractuale cu Universitatea.
- Pentru fiecare spaţiu cu acces restricţionat trebuie desemnată o persoană care să verifice periodic înregistrările de acces şi să cerceteze orice acces suspect.
- Accesul restricţionat trebuie marcat.

6. Regulament de Acces la Reţeaua de Comunicaţii

- Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către CIC.
- Departamentele şi Facultăţile trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RIC ale Universităţii. 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 CIC.
- Conectarea sistemelor de calcul care nu sunt proprietatea Universităţii se face numai cu aprobarea în scris a CIC la recomandarea Departamentelor sau a Facultăţilor.
- Accesul de la distanţă la reţeaua Universităţii se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către Universitate şi folosind protocoale aprobate de către CIC.
- Utilizatorii RIC din interiorul Universităţii nu se pot conecta la altă reţea.
- Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel (pe nici o cale). Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Facultăţilor şi a Departamentelor de către CIC.
- Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea CIC.
- Sistemele computerizate din afara Universităţii care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale Universităţii.
- 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 Universităţii nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua Universităţii. .

- Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.
- Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către CIC.
- Serviciile de interconectare a reţelei Universităţii cu alte reţele sunt realizate exclusiv de către CIC.
- Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea CIC. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către CIC.

7. Regulament privind Configurarea Sistemelor Informatice pentru Acces la Reţeaua de Comunicaţii

- Infrastructura de comunicaţii, reţeaua de comunicaţii digitale, a Universităţii este administrată de către CIC, care este responsabil cu întreţinerea şi dezvoltarea acesteia.
- Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare toate componentele acesteia sunt instalate de către CIC sau de către un furnizor avizat explicit de către CIC.
- Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor CIC.
- Orice dispozitiv hardware, inclusiv plăcile de reţea, care se va conecta la reţeaua Universităţii , trebuie să fie însoţit de o aprobare de tip (producător, model etc.) din partea CIC. Lista cu dispozitivele care pot fi conectate la reţeaua de comunicaţii a Universităţii va fi publicată pe site-ul web al CIC.
- Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai cu aprobarea CIC.
- Infrastructura de comunicaţii de date a Universităţii suportă un set definit de protocoale de reţea (TCP/IP). Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către CIC.
- Adresele de reţea sunt alocate dinamic sau static numai de către CIC.
- Toate conectările în reţeaua de comunicaţii a Universităţii sunt responsabilitatea CIC, conectarea se va face numai în baza unei cereri standard aprobată de către Departament sau Facultate şi de către conducerea Universităţii. Formularele vor fi puse la dispoziţie prin intermediul site-ului web al CIC.
- Toate conectările dintre reţeaua de comunicaţii a Universităţii şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a CIC.
- Echipamentele de protecţie a reţelei de comunicaţie a Universităţii (firewall) se vor instala de către CIC.
- Utilizarea sistemelor de protecţie (firewall) din Departamente şi Facultăţi nu este permisă fără autorizaţie scrisă din partea CIC. Această restricţie se aplică şi în cazul în care se folosesc adrese private de reţea.

- Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei (este interzisă instalarea unui telefon, fax, modem, router, switch, hub sau punct de acces la reţeaua Universităţii) fără aprobare din partea CIC.
- Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau programe care furnizează servicii de reţea fără aprobarea CIC.
- Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

8. Regulament de Tratare a Incidentelor de Securitate

- Membrii CIC in cazul incidentelor de securitate din Universitate au funcţii şi responsabilităţi predefinite care pot fi prioritare îndatoririlor obişnuite.
- Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc., trebuie urmate procedurile standard specifice pentru micşorarea riscurilor.
- CIC este responsabil cu înştiinţarea şi coordonarea pentru tratarea incidentului.
- CIC este responsabil cu strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului.
- Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităţilor acolo unde este cazul.
- CIC va stabili conţinutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informaţii.
- CIC trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.
- CIC este responsabil cu documentarea anchetei privind incidental.
- CIC este responsabil de coordonarea activităţilor de comunicare cu terţi pentru rezolvarea incidentului.
- În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare CIC va recomanda sancţiuni disciplinare.
- În cazul în care incidentul implică aplicarea legilor civile sau penale CIC va recomanda sesizarea organelor în drept ale statului şi va acţiona ca ofiţer de legătură cu acestea.

9. Regulament de Monitorizare a RIC

- Monitorizarea RIC se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice şi a situaţiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări şi înregistra:
    - Tipul traficului (ex. structura pe protocoale şi servicii) extern şi conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
    - Tipul traficului în reţeaua de campus, a protocoalelor şi a echipamentelor conectate la RIC, conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
    - Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

- Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale Universităţii. În această categorie intră următoarele (fără a se limita doar la acestea):
  - Jurnale ale sistemelor de detectarea automată a intruşilor;
  - Jurnale Firewall;
  - Jurnale ale activităţii conturilor utilizator;
  - Jurnale ale scanărilor reţea;
  - Jurnale ale aplicaţiilor;
  - Jurnale ale solicitărilor de suport tehnic;
  - Jurnale ale erorilor din sisteme şi servere.
- În mod regulat (cel puţin o dată la şase luni) se vor efectua verificări, de către CIC sau personalul autorizat al Departamentelor sau Facultăţilor pentru detectarea:
  - Parolelor utilizator care nu respectă regulamentele;
  - Echipamentelor de reţea conectate neautorizat;
  - Serviciilor de reţea neautorizate;
  - Serverelor de pagini de web neautorizate;
  - Echipamentelor ce utilizează resurse comune nesecurizate;
  - Utilizării de modemuri neautorizate;
  - Licenţelor pentru sistemele de operare şi programele instalate.
- Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către CIC în scopul efectuării de investigaţii.

10. Regulament de Securizare a Serverelor

- Un server nu trebuie conectat la reţeaua Universităţii până când nu se află într-o stare sigură acreditată de către CIC.
- Procedura de securizare a serverelor trebuie să includă obligatoriu următoarele:
  - Instalarea sistemului de operare dintr-o sursă aprobată;
  - Aplicarea patch-urilor furnizate de producător;
  - Inlăturarea programelor, a serviciilor sistem şi a driver-lor care nu sunt necesare;
  - Setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;
  - Dezactivarea sau schimbarea parolelor conturilor predefinite;
  - Securizarea accesului fizic la aceste echipamente.
- CIC va monitoriza obligatoriu pentru serverele principale (enterprise) procesul de instalare şi aplicare regulată a patch-urilor de securitate şi, prin sondaj, pentru serverele departamentale sau a grupurilor de lucru.

11. Regulament privind Crearea şi Utilizarea Copiilor de Siguranţă (Backup)

- Frecvenţa, dimensiunea şi conţinutul copiilor de siguranţă trebuie să fie în concordanţă cu importanţa informaţiei şi cu riscul acceptat de proprietarul datelor.
- Procedura de creare a copiilor de siguranţă şi de recuperare pentru fiecare sistem din cadrul RIC trebuie să fie documentată şi periodic revizuită.

- Furnizorul care oferă servicii de stocare a copiilor de siguranţă în alte zone pentru Universitate trebuie să fie acreditat în acest scop de către o autoritate a statului.
- Procedurile stabilite între Universitate şi furnizorii de stocare a copiilor de siguranţă în altă zonă trebuie să fie revizuite cel puţin anual.
- Verificarea copiilor de siguranţă se va face după o procedură documentată şi revizuită periodic.
- Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţiile stocate sunt recuperabile.
- Accesul la mediile de *backup* ale Universităţii stocate la furnizori externi sau în interior se va face folosind card-urile sau proceduri specifice de acces. Acestea trebuie revizuite periodic (anual). Accesul trebuie interzis pentru persoanele autorizate care îşi schimbă locul de muncă.
- 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.

12. Regulament pentru Detectarea Accesului Neautorizat

- 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).
- Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la reţea.
- Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.
- Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către administratorul de sistem.
- 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.
- Înregistrările de verificare pentru serverele şi host-urile din reţeaua internă trebuie revizuite cel puţin săptămânal.
- Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces neautorizat.
- Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.
- Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către CIC.
- Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile infracţiuni la CIC.

13. Regulamentul privind Securitatea Informaţiilor în cazul utilizării Calculatoarelor Portabile

- Calculatoarele portabile trebuie să fie protejate prin parole.
- Se va evita stocarea datelor care privesc Universitatea pe dispozitivele portabile. În cazul în care nu există o altă alternativă de stocare locală, toate datele care privesc Universitatea trebuie criptate utilizând tehnici aprobate.
- Transmiterea datelor prin reţele de tip wireless se poate face numai prin reţelele instalate de către CIC; acestea vor utiliza tehnici de criptare pentru protejarea datelor transmise.
- Toate accesările de la distanţă a RIC trebuie să se efectueze prin intermediul serviciului autorizat conform Regulamentului privind Securitatea Accesului la Reţea.
- Conectarea sistemelor de calcul care nu sunt proprietatea Universităţii se face numai cu aprobarea în scris a CIC la recomandarea Departamentelor sau a Facultăţilor.

14. Regulament pentru Modificări şi Modernizări ale RIC

- Orice modificare asupra unei componente a RIC din cadrul Universităţii, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă prezentului regulament şi trebuie să urmeze procedurile în vigoare.
- 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 Facultatea care administrează resursele afectate.
- Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RIC vor fi documentate şi aprobate de către CIC. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RIC.
- Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducerea Departamentului sau Facultăţii.
- Orice cerere de modificare planificată trebuie să obţină o aprobare formală din partea Departamentului sau Facultăţii care administrează resursele supuse modificărilor.
- Modificările planificate trebuie anunţate cu cel putin 48 ore înainte de a fi executate.
- 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.
- Se va întocmi un raport pentru orice modificare, indiferent dacă a fost planificată sau neplanificată, sau dacă s-a realizat sau nu cu succes.
- 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.

15. Regulament de Utilizare a reţelei Internet şi Intranet

- Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopuri academice şi de cercetare.
- Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către CIC. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie de către producător.
- Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore.
- Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy şi/sau firewall.
- Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze Regulamentului de Utilizare Acceptabilă a RIC.
- Orice activitate a utilizatorilor folosind RIC poate fi înregistrată şi ulterior examinată.
- Conţinutul tuturor site-urilor web ale Universităţii trebuie să se conformeze Regulamentelor de Utilizare Acceptabilă a RIC şi să folosească numele de domeniu al Universităţii (usamvcluj.ro).
- Nu se vor publica pe site-urile web ale Universităţii materiale cu caracter ofensiv sau de hărţuire.
- Nu se vor publica pe site-urile web ale Universităţii materiale publicitare comerciale sau personale.
- Nu este permisă utilizarea RIC ale Universităţii în scop personal sau pentru solicitări personale ce nu au legătură cu Universitatea.
- Cumpărăturile pe Internet care nu au legătură cu atribuţiile de serviciu sunt interzise. Cumpărăturile în interes de serviciu se vor supune regulilor de achiziţie ale Universităţii.
- Orice material confidenţial al Universităţii transmis prin reţeaua Internet trebuie criptat.
- Fişierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente şi regulamentele proprii fiecărui Departament sau Facultate.

16. Regulament de Administrare a Conturilor

- Toate conturile create trebuie să aibă asociată o cerere şi o aprobare corespunzătoare.
- Toate conturile utilizator se vor crea în formatul Prenume.Nume.
- Prin contractul de muncă, contractul de şcolarizare şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului RIC.

- Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.
- Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.
- Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Regulamentul privind Parolele de Acces.
- Toate conturile utilizator care nu au fost accesate timp de 90 de zile vor fi dezactivate. După încă 90 zile conturile vor fi şterse dacă nu s-a solicitat accesul la acestea.
- CIC rebuie să aibă o documentaţie de modificare a conturilor utilizator pentru a se pune de acord în situaţii precum schimbări ale numelor de familie, modificări privind contul (numele contului) modificări ale drepturilor de utilizator.
- CIC trebuie să furnizeze o listă cu toţi utilizatorii (listă de conturi) pentru sistemele pe care le administrează, la cererea conducerii autorizate din Universitate.

17. Reguli pentru Parolele de Acces

- Toate parolele trebuie să îndeplinească următoarele condiţii:
  - Să fie schimbate de utilizator în mod regulat, cel puţin o dată la 45 de zile;
  - Să aibă o lungime minimă de 8 caractere;
  - Să fie parole complexe;
  - Reutilizarea parolelor este interzisă;
  - Parolele stocate trebuie criptate;
  - Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice.
- Dispozitivele de securitate (ex. card Smart) trebuie returnate după terminarea relaţiilor cu Universitatea.
- Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.
- Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.
- Utilizatorii nu pot folosi programe de stocare a parolelor. Se pot face excepţii pentru anumite aplicaţii (precum backup automat) cu aprobarea CIC. Pentru ca o excepţie să fie aprobată, trebuie să existe o procedură pentru schimbarea parolelor.
- 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.
- Procedurile de schimbare a parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:
  - Utilizatorul se va legitima, administratorul va verifica drepturile de acces a persoanei la contul utilizator;
  - Se va genera o parolă care va fi comunicată utilizatorului;
  - Utilizatorul va schimba parola temporară, comunicată anterior, în maxim 24 ore.

18. Regulament privind Sistemul de Mesagerie Electronică

- Următoarele activităţi sunt interzise de regulament:
  - 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.
- Următoarele activităţi sunt 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.
- Toate informaţiile şi datele confidenţiale ale Universităţii, transmise către alte reţele externe, trebuie să fie criptate.
- Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea RIC ale Universităţii 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 Universităţii 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 Universitatea. Un exemplu de declaraţie simplă este: "părerile exprimate sunt personale, şi nu ale Universităţii … ".
- Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informaţii confidenţiale sau nesigure, ce privesc Universitatea, folosind dispozitive de comunicaţii mobile care nu sunt autorizate de Universitatea. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenţi digitali personali, pagere ce permit trimiterea/primirea de informaţii şi telefoanele mobile.

19. Regulament de Detectare a Viruşilor

- Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Universităţii, trebuie să utilizeze programe antivirus aprobate de către CIC.
- Programele antivirus nu trebuie dezactivate.
- Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.
- Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

- 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.
- Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat şi trebuie să respecte regulile de instalare şi utilizare a acestui program.
- Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat CIC.

20. Regulament de Relaţii cu Terţi

- Orice activitate desfăşurată de furnizor care implică acces la RIC trebuie să se conformeze cu regulamentele în vigoare ale Universităţii, cu procedurile standard şi convenţiile care cuprind, dar nu se limitează la următoarele:
  - Regulamente de Securitate a Accesului Fizic;
  - Regulamente de Confidenţialitate;
  - Regulamente de Securitate a Accesului la RIC;
  - Regulamente de Modificare şi Modernizare;
  - Regulament de Utilizare Acceptabilă.
- În toate convenţiile şi contractele încheiate cu Furnizori trebuie specificate următoarele:
  - Informaţiile din cadrul Universităţii, 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 Universităţii aflate în posesia Furnizorului, la încheierea contractului.
- Furnizorul trebuie să folosească sistemul RIC din cadrul Universităţii numai în scopul stipulat în contract.
- Orice altă informaţie din sistemul RIC al Universităţii obţinută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.
- Toate echipamentele de întreţinere ale Furnizorului, aflate în reţeaua internă a Universităţii şi care se pot conecta în exterior prin intermediul reţelei, a liniilor telefonice sau a liniilor închiriate, precum şi toate conturile de utilizator create temporar pentru Furnizor şi necesare pentru acces la RIC ale Universităţii, vor fi scoase din uz la încheierea relaţiilor contractuale.
- Accesul Furnizorului trebuie să fie identificat în mod unic, iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu Regulamentul privind Parolele de Acces ale Universităţii şi Regulamentul de Acces Administrativ.
- Activităţile principale ale Furnizorului trebuie să fie documentate de acesta şi puse la dispoziţia conducerii Universităţii, la cerere. Acestea trebuie să cuprindă, dar să nu fie limitate la, evenimente precum: schimbări de personal, schimbări de parolă, schimbări majore în derularea proiectului, timpii de sosire, de plecare şi de livrare.

- În cazul retragerii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informaţiile sensibile sunt colectate şi predate Universităţii sau distruse în cel mult 24 de ore de la producerea evenimentului.
- În cazul terminării/rezilierii contractului sau la cererea Universităţii, Furnizorul va preda sau distruge toate informaţiile ce aparţin Universităţii şi va oferi certificare în scris privind predarea sau distrugerea informaţiilor în decurs de 24 de ore de la producerea evenimentului.
- În cazul încheierii contractului sau la cererea Universităţii, Furnizorul trebuie să predea imediat toate legitimaţiile, cartelele de acces, echipamentele şi stocurile Universităţii. Echipamentele şi/sau stocurile care urmează a fi reţinute de către Furnizor trebuie documentate şi autorizate de Conducerea Universităţii.
- Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către Universitatea trebuie să fie inventariate corespunzător şi să posede drepturi de utilizare atestate prin Licenţe.