Plan de Securitate
Utilizarea Resurselor Informatice şi de Comunicații
Universitatea „Alexandru Ioan Cuza” din Iaşi

Introducere	Regulamentele de Utilizare a Resurselor Informatice şi de Comunicații sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informației şi comunicațiilor în Universitatea “Alexandru Ioan Cuza” din Iaşi. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea acestea au ca scop protejarea imaginii Universității şi a investițiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicații
Scop	În acord cu legislația în vigoare în România, Regulamentele de ordine interioară ale Universității Alexandru Ioan Cuza Iaşi, Resursele Informatice şi de Comunicații sunt valori ale Universității Alexandru Ioan Cuza Iaşi care trebuie exploatate şi administrate ca resurse publice în proprietatea statului român. Scopul acestor regulamente este acela de a asigura: 1. Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicații în vederea sprijinirii procesului educațional şi a cercetării ştiințifice; 2. Protejarea imaginii Universității “Alexandru Ioan Cuza” din Iaşi; 3. Protejarea investițiilor Universității “Alexandru Ioan Cuza” din Iaşi pentru dezvoltarea sistemului informatic şi de comunicații propriu; 4. Protejarea proprietății intelectuale şi a tuturor informațiilor stocate şi transportate folosind Resursele Informatice şi de Comunicații ale utilizatorilor autorizați: cadre didactice, personal administrativ, studenți, colaboratori etc. 5. Educarea utilizatorilor resurselor informatice şi de comunicații în ceea ce priveşte responsabilitățile asociate cu utilizarea acestora; 6. Compatibilitate cu regulamentele, statutul şi atribuțiile stabilite pentru administrarea resurselor informatice şi de comunicații.
Audiență	Planul de Securitate privind utilizarea resurselor informatice şi de comunicații ale Universității Alexandru Ioan Cuza Iaşi se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acesta.
Proceduri de elaborare, modificare şi aprobare a Regulamentelor	1. Regulamentele şi/sau procedurile de utilizare a Resurselor Informatice şi de Comunicații ale Universității “Alexandru Ioan Cuza” din Iaşi se elaborează pentru fiecare activitate specifică domeniului şi trebuie concepute în aşa fel încât fiecare Regulament să poată fi folosit cvasi-independent de celelalte. 2. Regulamentele vor fi elaborate de către Departamentul de

	Comunicaţii Digitale şi vor fi propuse pentru aprobare conducerii Universităţii “Alexandru Ioan Cuza” din Iaşi. 3. Prevederile Politicii de Securitate aprobate vor fi incluse în contractul de munca, contractul cu studenţii şi toate contractele cu terţi (dacă activitatea acestora are legătură cu sistemul Resurselor Informatice şi de Comunicaţii al Universităţii) şi face referire la Planul de Securitate 4. 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. 5. Regulamentele de utilizare a sistemului Resurselor Informatice şi de Comunicaţii vor fi disponibile în format electronic pe sit-ul web al Universităţii “Alexandru Ioan Cuza” din Iaşi şi pe sit-ul web al Departamentului de Comunicaţii Digitale. Se recomandă ca aceste documente să fie disponibile sau să se facă trimitere la acestea de pe toate sit-urile web din cadrul Universităţii “Alexandru Ioan Cuza” din Iaşi 6. Modificarea prevederilor unui Regulament se face cu aprobarea conducerii Universităţii „Alexandru Ioan Cuza” din Iaşi. Fiecare modificare va include modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea anterioara rămâne valabilă până în momentul în care noua versiune este aplicabilă. 7. Prezentul document va fi conţine o listă a tuturor regulamentelor aplicabile în sistemul Resurselor Informatice şi de Comunicaţii.

Proceduri şi Regulamente Specifice

Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.

1. Utilizare Acceptabilă a Resurselor Informatice şi de Comunicații

Introducere	În acord cu prevederile Politicii de Securitate, Resursele Informatice şi de Comunicații (RIC) sunt bunuri strategice ale Universității „Alexandru Ioan Cuza” din Iaşi care trebuiesc administrate ca resurse ale statului român. Acest regulament este stabilit astfel încât: 1. Să fie în conformitate cu Politica de Securitate, statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice publice, 2. Să stabilească practici prudente şi acceptabile privind utilizarea RIC ale Universității “Alexandru Ioan Cuza” din Iaşi, 3. Să instruiască utilizatorii care au dreptul de folosire a RIC privind responsabilitățile lor asociate unei astfel de utilizări.
Audiență	Regulamentul de Utilizare Acceptabilă a Resurselor Informatice şi de Comunicații al Universității „Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicații a Universității „Alexandru Ioan Cuza” din Iaşi.
Confidențialitate	Fişierele electronice create, trimise, primite sau stocate pe Resurse Informatice proprii , închiriate, administrate sau în custodia şi sub controlul Universității „Alexandru Ioan Cuza” din Iaşi, nu sunt confidențiale şi pot fi accesate de către personalul responsabil cu securitatea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi, oricând fără înştiințarea utilizatorului sau a Departamentului sau Facultății care are în gestiune sistemul. Conținutul unui fişier electronic poate fi accesat de către personalul autorizat în conformitate cu prevederile şi normele de securitate ce se regăsesc în Regulamentul de Acces Administrativ.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: *mainframe*-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi

	utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universităţii, titlul este atribuit în mod automat Rectorului Universităţii Alexandru Ioan Cuza Iaşi. *Ofițer responsabil cu Securitatea RIC (OSRIC):* Răspunde în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Universității “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universităţii “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcția OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcția de OSRIC, persoană care trebuie validată de către ARIC . *Ofițer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății şi validat de către OSRIC. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Abuz de privilegii*: Orice acțiune întreprinsă în mod voit de un utilizator, care vine in contradicție cu regulamentele Universității “Alexandru Ioan Cuza” si/sau legile in vigoare, inclusiv cazul in care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acțiunii respective. *Furnizor*: Persoană fizică/juridică care oferă bunuri sau servicii Universității “Alexandru Ioan Cuza” din Iaşi în baza unui contract comercial sau de colaborare.
Regulament de Utilizare Acceptabilă a RIC	1. Utilizatorii trebuie să anunțe OSRIC sau OSRICD în cazul în care se observă orice problemă/breşă în sistemul de securitate a RIC din cadrul Universității “Alexandru Ioan Cuza” din Iaşi cât şi orice posibilă întrebuințare greşită sau încălcare a regulamentelor în vigoare. 2. Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea şi disponibilitatea informațiilor de orice tip în cadrul sistemului RIC al Universității „Alexandru Ioan Cuza” din Iaşi. 3. Utilizatorii nu trebuie să încerce să obțină acces la date sau programe din RIC pentru care nu au autorizație sau consimțământ explicit. 4. Utilizatorii nu trebuie să divulge nimănui numerele de acces Dialup sau Dialback prin modem. 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 si/sau informații similare utilizate în scopuri de autorizare şi identificare. 6. Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright). 7. Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea OSRIC, cu excepția cazului în care acestea se găsesc pe lista programelor standard folosite în cadrul Universității “Alexandru Ioan Cuza” din Iaşi. Această listă va fi întocmită de către

	Departamente şi Facultăţi, aprobată de către OSRIC şi publicată de către Departamente şi Facultăţi. 8. Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane; să degradeze performanţele RIC; să împiedice accesul unui utilizator autorizat la RIC; să obţină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente. 9. Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii RIC. De exemplu, utilizatorii Universităţii „Alexandru Ioan Cuza” nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente. 10. RIC ale Universităţii “Alexandru Ioan Cuza” din Iaşi. nu trebuiesc folosite pentru beneficiul personal. 11. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Universitatea „Alexandru Ioan Cuza” 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) 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. Angajaţii nu trebuie să permită membrilor familiei sau altor persoane accesul la RIC ale Universităţii „Alexandru Ioan Cuza Iaşi”. 13. Utilizatorii care au acces la sistemul RIC al Universităţii „Alexandru Ioan Cuza” din Iaşi au obligaţia de a purta acte şi sau legitimaţii care să ateste calitatea de utilizator autorizat în spaţiile Universităţii „Alexandru Ioan Cuza” din Iaşi. 14. Utilizatorii vor folosi, exclusiv, numele de domeniu (uaic.ro) în toate activităţile desfăşurate prin intermediul sau folosind sistemul RIC al Universităţii „Alexandru Ioan Cuza”. Utilizarea denumirilor pentru calculatoare şi a adreselor de e-mail care nu au sufixul uaic.ro este strict interzisă. 15. Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor Universităţii “Alexandru Ioan Cuza” din Iaşi folosind RIC.
Utilizare Ocazională	În anumite situaţii este permisă utilizarea ocazională a RIC. În aceste situaţii se aplică următoarele restricţii: 1. Utilizarea personală ocazională a serviciilor de poştă electronică, acces internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricţionată la utilizatorii autorizaţi şi nu poate fi extinsă la membrii familiilor sau alte persoane. 2. Utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru Universitatea Alexandru Ioan Cuza Iaşi. 3. Utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaţilor. 4. Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Universităţii Alexandru Ioan Cuza Iaşi sau prejudicierea, indiferent de formă, a intereselor Universităţii. 5. Stocarea mesajelor de email, a mesajelor de voce, a documentelor şi

	fişierelor personale din cadrul RIC trebuie să fie nominală. 6. Toate mesajele, fişierele şi documentele – incluzând mesajele personale, fişierele şi documentele – localizate în cadrul RIC sunt proprietatea Universităţii şi pot fi subiectul unor cereri de verificare/inspectare/accesare conform regulamentelor.
Măsuri Disciplinare	Încălcarea acestui regulament se sancţionează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaţilor, 2. Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenţilor, 4. Interzicerea accesului la sistemul RIC, Toate acţiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziţii	Acest Regulament are ca parte integranta următoarele dispoziţii: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct responsabil pentru acţiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Utilizarea RIC se face numai în interes de serviciu. 4. 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. 5. Departamentele şi facultăţile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 6. 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. 7. Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele trebuie protejate fiind proprietatea Universităţii. 8. Departamentele şi Facultăţile 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. 9. 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. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din

	cadrul RIC. 10. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fişiere, dar nu limitate la: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip *freeware* şi *shareware*.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.

2. Declarații privind Confidențialitatea Serviciilor Informatice şi de Comunicații

Introducere	Regulamentele de Confidențialitate sunt mecanisme utilizate pentru a stabili limite pentru utilizatorii RIC. Utilizatorii interni nu ar trebui să se aştepte la confidențialitate în ceea ce priveşte utilizarea sistemului RIC. Utilizatorii externi ar trebui să se aştepte la confidențialitate totală, cu excepția cazului în care se suspectează un delict cu privire la sistemul RIC.
Scop	Scopul Regulamentului privind Confidențialitatea Serviciilor Informatice şi de Comunicații ale Universității “Alexandru Ioan Cuza” din Iaşi este acela de a comunica în mod clar utilizatorilor la ce să se aştepte în ceea ce priveşte confidențialitatea datelor stocate în sistemul RIC.
Audiență	Regulamentul privind Confidențialitatea Serviciilor Informatice şi de Comunicații al Universității „Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicații a Universității „Alexandru Ioan Cuza” din Iaşi.
Drept de Proprietate	Fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea, sau în custodia şi sub controlul Universității „Alexandru Ioan Cuza”, sunt proprietatea Universității în condițiile legilor în vigoare.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iaşi. *Ofițer responsabil cu Securitatea RIC (OSRIC):* Răspunde în fața ARIC

	privind administrarea funcţiilor de securitate a informaţiei în cadrul Universităţii “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universităţii “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcţia OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC . *Ofiţer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăţi. Acesta este desemnat de către conducătorul Departamentului/Facultăţii şi validat de către OSRIC. *Utilizator:* O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Server Web:* un sistem de calcul care distribuie în mod public sau diferenţiat informaţii folosind protocolul HTTP. *Pagină web*: Un document în spaţiul World Wide Web (WWW). Fiecare pagină *web* este identificată printr-un URL (Uniform Resource Locator).
Regulament privind Confidenţialitatea Serviciilor Informatice şi de Comunicaţii	1. Fişierele electronice create, trimise, primite sau stocate folosind sistemul RIC proprii, administrate sau în custodia şi sub controlul Universităţii „Alexandru Ioan Cuza” nu sunt confidenţiale şi pot fi accesate oricând de către angajaţii autorizaţi din cadrul D.C.D., Departamente şi Facultăţi fără înştiinţarea utilizatorului conform Regulamentului de Acces Administrativ. 2. În scopul administrării RIC şi pentru asigurarea securităţii RIC personalul autorizat poate revizui sau utiliza orice informaţie stocată pe sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor (de exemplu, dar fără a se limita la, numere de telefon formate sau sit-uri web vizitate). 3. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Universităţii “Alexandru Ioan Cuza”, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea OSRIC sau OSRICD). 4. Un mare număr de utilizatori (inclusiv studenţi), pot accesa informaţii din exteriorul sistemului de comunicaţii al Universităţii „Alexandru Ioan Cuza” din Iaşi. În aceste condiţii este obligatorie păstrarea confidenţialităţii informaţiilor transmise din exteriorul RIC şi a informaţiilor obţinute din interior. 5. Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Universităţii “Alexandru Ioan Cuza” din Iaşi pentru care nu au autorizaţie sau consimţământ explicit. 6. Nici un utilizator al sistemului RIC ale Universităţii “Alexandru Ioan Cuza” din Iaşi 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 “Alexandru Ioan Cuza” din Iaşi. 7. Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicaţii ale terţilor nu poate fi asigurată. Pentru aceste situaţii, confidenţialitatea şi integritatea informaţiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligaţi să se asigure că toate

	informaţiile confidenţiale ale Universităţii „Alexandru Ioan Cuza” din Iaşi se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.
Regulament pentru Accesul Publicului la Informaţii	Modelul de mai jos trebuie folosit pentru toate cazurile în care prin sistemul RIC se oferă informaţii publicului. Sit-urile web ale Universităţii “Alexandru Ioan Cuza” disponibile publicului general trebuie să conţină o declaraţie prin care se atenţionează vizitatorii privind confidenţialitatea acţiunilor lor. Un exemplu bun de Declaraţie este următorul: *Următoarea declaraţie se aplică numai publicului şi este destinată atenţionării acestuia cu privire la informaţiile înregistrate cu ocazia accesării informaţiei din sistemul Resurselor Informatice şi de Comunicaţii al Universităţii “Alexandru Ioan Cuza” din Iaşi.* *Cookie-uri: Un „cookie” este un fişier care conţine informaţie plasată de către un server web pe un calculator al utilizatorului. De obicei, aceste fişiere sunt utilizate pentru a facilita accesul la informaţia oferită de sit-ul web. Orice informaţie pe care serverele web ale Universităţii „Alexandru Ioan Cuza” o pot stoca în cookie-uri este utilizată numai în interiorul Universităţii “Alexandru Ioan Cuza” din Iaşi. Informaţia din cookie-uri nu este utilizată pentru a dezvălui, către terţi, informaţii despre vizitator decât în cazul în care Universităţii „Alexandru Ioan Cuza” din Iaşi i se cere în mod legal să facă acest lucru în conformitate cu legile în vigoare sau alte proceduri legale.* *Jurnale şi Monitorizare: Universitatea „Alexandru Ioan Cuza” păstrează fişierele cu înregistrări ale tuturor accesărilor sit-urilor sale şi de asemenea monitorizează traficul din reţea în scopul administrării sit-urilor. Această informaţie este utilizată pentru a ajuta la diagnosticarea eventualelor probleme şi pentru a realiza alte sarcini administrative. Uneltele de analiză a jurnalelor sunt de asemenea utilizate pentru statistici în scopul determinării informaţiei cu un grad ridicat de interes pentru utilizatori sau vizitatori.* *Informaţiile incluse în aceste fişiere sunt:* • *Numele sistemului: numele sistemului şi/sau adresa IP a calculatorului care cere accesarea sit-ului.* • *Agent-Utilizator: tipul browser-ului, versiunea, şi sistemul de operare al calculatorului care cere accesarea site-ului (Netscape 4 for Windows, IE 4 for Macintosh, etc.)* • *Referinţă: pagina web de unde a venit utilizatorul* • *Data sistemului: data şi ora accesării* • *Cerere completă: cererea exactă făcută de utilizator* • *Stare: codul de stare returnat de server, ex: “file not found” (nu a găsit fişierul)* • *Mărimea conţinutului: lungimea, în bytes (octeţi), a fişierului trimis utilizatorului* • *Metodă: metoda cererii folosită de către browser (ex.: post, get)* • *Uniform Resource Identifier (URI): adresa unei anumite resurse cerute.* • *Şir de interogare din URI: orice după un semn de întrebare în cadrul unui URI. De exemplu, dacă a fost cerut un cuvând cheie de căutare, acel cuvânt cheie va apare în şirul interogării.* • *Protocol: protocolul tehnic şi versiunea utilizată, de ex.: http 1.0, ftp, etc.* *Informaţia de mai sus nu va fi folosită pe nici o cale care ar putea dezvălui informaţie de identificare personală unei persoane din exteriorul Universităţii “Alexandru Ioan Cuza” din Iaşi, decât dacă se cere în mod legal acest lucru în conformitate cu legile în vigoare sau cu alte proceduri legale.* *Informaţie din mesaje electronice sau formulare: Dacă un vizitator trimite un mesaj electronic Universităţii „Alexandru Ioan Cuza” sau completează un formular web cu*

	o întrebare sau comentariu ce conține informație de identificare personală, acea informație va fi utilizată numai pentru a răspunde cererii şi pentru a analiza intențiile. Mesajul poate fi redirectat la altă persoană care este calificată să răspundă cererii. Astfel de informații nu vor fi folosite pe nici o cale prin care s-ar dezvălui informație de identificare personală terților, cu excepția cazului în care Universității i se cere în mod legal acest lucru în conformitate cu legile în vigoare sau cu alte proceduri legale. *Legături: Acest sit poate conține legături la alte sit-uri. Universitatea „Alexandru Ioan Cuza” nu este răspunzătoare de politicile de securitate sau conținutul acestor sit-uri.* *Contact: Dacă aveți întrebări în legătură cu această declarație sau utilizarea acestui site vă rugăm să contactați: [Informație de contact]*
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integrantă următoarele dispoziții: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct responsabil pentru acțiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili, nediscriminatoriu, privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Utilizarea RIC se face numai în interes de serviciu. 4. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare. 5. Departamentele şi facultățile sunt responsabile cu autorizarea utilizatorilor pentru folosirea adecvată a RIC. 6. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar. 7. Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația şi datele trebuie protejate fiind proprietatea Universității. 8. Departamentele şi Facultățile trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării RIC pentru protejare datelor şi programelor împotriva întrebuințării greşite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător.
Referințe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt

	2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

3. Acces Administrativ

Introducere	Personalul care asigură suport tehnic, OSRIC, OSRICD, administratorii de sistem şi alte persoane pot avea conturi cu drepturi de acces privilegiat în comparație cu utilizatorii obişnuiți. Datorită faptului că aceste conturi pentru acces administrativ au mai multe privilegii aprobarea, verificarea şi monitorizarea acestora sunt extrem de importante din punctul de vedere al securității RIC.
Scop	Scopul Regulamentului de Acces Administrativ al Universității “Alexandru Ioan Cuza” din Iaşi, este de a stabili regulile pentru crearea, utilizarea, monitorizarea, controlarea şi ştergerea conturilor cu drepturi speciale de acces.
Audiență	Procedura de Acces Administrativ se aplică nediscriminatoriu tuturor persoanelor care au sau pot cere şi obțin drepturi speciale de acces la orice RIC a Universității “Alexandru Ioan Cuza”.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iaşi. *Ofițer responsabil cu Securitatea RIC (OSRIC):* Răspunde în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Universității “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universității “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcția OSRIC este asumată de către şeful Departamentului de Comunicații Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcția de OSRIC, persoană care trebuie validată de către ARIC . *Ofițer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):*

	Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății şi validat de către OSRIC. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare să folosească RIC. *Abuz de privilegii*: Orice acțiune întreprinsă în mod voit de un utilizator, care vine in contradicție cu regulamentele Universității “Alexandru Ioan Cuza” si/sau legile in vigoare, inclusiv cazul in care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acțiunii respective. *Furnizor*: Persoană fizică/juridică care oferă bunuri sau servicii Universității “Alexandru Ioan Cuza” din Iaşi în baza unui contract comercial sau de colaborare..
Regulament de Acces Administrativ	1. Departamentele şi Facultățile Universității “Alexandru Ioan Cuza” din Iaşi trebuie să prezinte la D.C.D. o listă cu informații de contact în plan administrativ pentru toate sistemele conectate rețeaua de comunicații a Universității. Această listă trebuie refăcută şi prezentată la D.C.D. 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 instrucțiuni de administrare, documentare, instruire şi autorizare a conturilor. Aceste instrucțiuni se vor elabora de către fiecare Departament sau Facultate şi vor fi incluse în fişa postului. 4. Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi şi trebuie să facă investigații numai sub îndrumarea OSRIC sau OSRICD. 5. Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activității pe care o desfăşoară. 6. Accesul administrativ trebuie să se conformeze Regulamentului de utilizare a Parolelor. 7. Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al OSRIC şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă din cadrul Departamentului, Facultății sau a Universității, sau în cazul unei modificări a listei de personal ale terților (furnizor desemnat) în contractele cu Universitatea “Alexandru Ioan Cuza” din Iaşi. 8. Trebuie să existe o procedură prin care o altă persoană, în afară de administrator, să poată avea acces la contul administratorului în caz de forța majoră. Această procedură va fi elaborată de către OSRICD pentru fiecare Facultate şi Departament şi va fi aprobată de către OSRIC. 9. Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operațiuni definite. Acestea trebuie sa îndeplinească următoarele condiții: • trebuie să fie autorizate ;

	• trebuiesc create cu dată de expirare specifică; • contul va fi şters atunci când nu mai este necesar.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integrantă următoarele dispoziții: 1. Controalele de Securitate ale Resurselor Informatice nu trebuie să fie ocolite sau dezactivate. 2. Accesul la, schimbarea şi utilizarea drepturilor de acces la RIC trebuie să fie strict securizate. Trebuiesc revizuite în mod regulat modul de autorizare a accesului la informație, drepturile de acces precum şi orice modificare a stării postului cum ar fi: transfer, promovare, retrogradare sau terminarea serviciului 3. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct responsabil pentru acțiunile care pot afecta securitatea RIC. 4. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 5. Utilizarea RIC se face numai în interes de serviciu. 6. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nu limitate la, mesagerie electronică, navigare Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare. 7. Departamentele şi Facultățile sunt responsabile privind autorizarea utilizatorilor pentru folosirea adecvată a RIC. 8. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar. 9. Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația şi datele trebuie protejate fiind proprietatea Universității. 10. Departamentele şi Facultățile trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării RIC în scopul protejării datelor şi programelor împotriva întrebuințării greşite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător. 11. Orice program comercial utilizat în cadrul RIC trebuie să fie însoțit de Licență care să specifice clar drepturile de utilizare şi restricțiile

	produsului. Personalul trebuie să respecte prevederile Licențelor si nu este permisă copierea şi distribuirea ilegală a softul cu licența. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăților, îşi rezervă dreptul de a şterge orice produs fără Licență de pe orice sistem din cadrul RIC. 12. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăților, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fişiere: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), pop email, fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip freeware şi shareware.
Referințe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

4. Accesul Fizic

Introducere	Ca parte a atribuțiilor de serviciu, personalul care asigură suport tehnic, administratorii de rețea, administratorii de sistem sau alte persoane autorizate trebuie să aibă acces la echipamentele şi componentele sistemului RIC. Procesul de control şi monitorizare a drepturilor de acces fizic la resursele RIC este important şi va fi reglementat conform prezentului regulament de către D.C.D. şi, acolo unde este cazul, de către fiecare Departament sau Facultate.
Scop	Scopul Regulamentului privind Accesul Fizic la RIC este stabilirea regulilor pentru acordarea, controlarea, monitorizarea şi întreruperea drepturilor de acces fizic la echipamentele componente ale RIC.
Audiență	Regulamentul privind Accesul Fizic la RIC se aplică tuturor persoanelor care răspund de buna funcționare a infrastructurii, instalarea şi întreținerea unor componente funcționale, a personalului responsabil cu securitatea RIC şi utilizatori.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iaşi. *Ofițer responsabil cu Securitatea RIC (OSRIC):* Răspunde în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Universității “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universității “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcția OSRIC este asumată de către şeful Departamentului de Comunicații Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcția de OSRIC, persoană care trebuie validată de către ARIC .

	Ofițer responsabil cu securitatea RIC la nivel Departamental: (OSRICD): Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății şi validat de către OSRIC. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC.
Regulament privind Accesul Fizic la RIC	1. 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 Universității “Alexandru Ioan Cuza” din Iaşi. 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 funcție de importanța 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 funcționare a echipamentelor din încăperea respectivă şi, dacă este cazul, părților contractante, ale căror obligații contractuale implică acces fizic. 5. Personalul care are drepturi de acces trebuie să dețină legitimație de serviciu şi acte de identitate care să-i ateste calitatea. 6. Acordarea drepturilor de acces (folosind card-uri, chei, parole, etc) se face în scris de către D.C.D. sau, după caz, Departamentul sau Facultatea care deține încăperea şi resursele. 7. Nu este permis transferul dreptului de acces indiferent de motiv. 8. Cardurile şi/sau cheile de acces care nu mai sunt folosite trebuie predate Departamentului sau Facultății care le-a eliberat. 9. Pierderea sau furtul cardurilor şi/sau cheilor de acces trebuie raportate imediat Departamentului sau Facultății care le-a eliberat. 10. Cardurile şi/sau cheile nu trebuie să aibă informații de identificare, altele decât informația de contact necesară pentru returnare. 11. Accesul vizitatorilor în spațiile protejate trebuie documentat pentru fiecare încăpere şi, în cazul în care este permis, se va delega un însoțitor. Vizitatorii trebuie să fie însoțiti în zonele cu acces restricționat. 12. Fiecare Departament şi Facultate va ține o evidență a tututor cardurilor şi/sau cheilor de acces emise, retrase, pierdute sau furate. 13. Pentru fiecare spațiu în care sunt instalate RIC se va păstra o evidență a accesului pentru verificări de rutină în situații critice. 14. Fiecare 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. 15. Fiecare Departament şi/sau Facultate trebuie să anuleze drepturile de acces ale cardurilor şi/sau cheilor utilizatorilor care îşi schimbă locul de muncă din Universitatea “Alexandru Ioan Cuza” din Iaşi sau nu au relații contractuale cu Universitatea. 16. Pentru fiecare spațiu cu acces restricționat trebuie desemnată o persoană care să verifice periodic înregistrările de acces şi să cerceteze orice acces suspect.

	17. Accesul restricționat trebuie marcat.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integranta următoarele dispoziții: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct responsabil pentru acțiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Utilizarea RIC se face numai în interes de serviciu. 4. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nu limitate la, poştă electronică, navigare pe Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare. 5. Departamentele şi facultățile sunt responsabile privind autorizarea utilizatorilor pentru folosirea adecvată a RIC. 6. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar. 7. Controalele de Securitate ale RIC nu trebuie să fie evitate sau dezactivate. 8. Parolele, Numerele de Identificare Personală, Cartelele de Acces precum şi alte proceduri de securitate a sistemelor de calcul sau a dispozitivelor din cadrul RIC trebuie să fie protejate de fiecare utilizator în parte astfel încât să nu poată fi utilizate de alți utilizatori. Orice încălcare a sistemului de securitate trebuie raportată OSRIC şi/sau OSRICD. 9. Accesul la RIC trebuie să fie strict securizat şi să se facă pe baza unor proceduri documentate conform prezentului regulament pentru fiecare Departament şi Facultate în parte. Aceste proceduri trebuie revizuite în mod regulat. 10. La terminarea relațiilor dintre utilizatorul RIC şi Universitatea “Alexandru Ioan Cuza” din Iaşi acesta trebuie sa predea toate componentele sistemului RIC de care răspunde sau le are în inventar. Toate regulile de securitate pentru sistemul RIC se aplică si rămân în vigoare şi după încheierea relațiilor dintre utilizator şi Universitatea “Alexandru Ioan Cuza”.

	11. Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele trebuie protejate fiind proprietatea Universităţii. 12. Departamentele şi Facultăţile trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIC în scopul 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. 13. Sistemele şi/sau echipamentele asociate RIC din cadrul Universităţii “Alexandru Ioan Cuza” din Iaşi utilizate pentru activităţile Universităţii care sunt dirijate, controlate sau administrate din exteriorul Universităţii trebuie sa îndeplinească cerinţe contractuale specifice si vor fi monitorizate în vederea respectării tuturor reglementărilor de securitate.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.

5. Conectarea la Sistemul Resurselor Informatice şi de Comunicații

Introducere	Rețeaua de comunicații a Universității “Alexandru Ioan Cuza” constituie unul din principalele mijloace de exploatare a resurselor informatice. Aceasta include toate echipamentele, cablurile, canalele de cabluri, punctele de acces, punctele de distribuție şi nodurile principale. Este important ca aceasta să se dezvolte controlat şi continuu în condiții de flexibilitate şi evolutivitate. Este important ca dezvoltarea rețelei de comunicații să se facă având în vedere atât cerințele utilizatorilor privind furnizarea de servicii avansate şi diferențiate cât şi cerințele privind securitatea întregului ansamblu.
Scop	Scopul Regulamentului de Acces la Rețeaua de Comunicații a Universității “Alexandru Ioan Cuza” din Iaşi constă în stabilirea regulilor de acces şi utilizare a acesteia. Aceste reguli sunt necesare pentru păstrarea integrității, disponibilității şi confidențialității informației din cadrul RIC ale Universitatea “Alexandru Ioan Cuza”.
Audiență	Regulamentul de Acces la Rețeaua de Comunicații a Universității “Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor utilizatorilor care au acces la orice RIC.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iaşi. *Ofițer responsabil cu Securitatea RIC (OSRIC):* Răspunde în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Universității “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universității “Alexandru Ioan Cuza” pentru orice problemă în

	legătură cu securitatea RIC. Funcţia OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC . *Ofiţer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăţi. Acesta este desemnat de către conducătorul Departamentului/Facultăţii şi validat de către OSRIC. *Utilizator:* O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Abuz de privilegii*: Orice acţiune întreprinsă în mod voit de un utilizator, care vine in contradicţie cu regulamentele Universităţii “Alexandru Ioan Cuza” si/sau legile in vigoare, inclusiv cazul in 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 Universităţii “Alexandru Ioan Cuza” din Iaşi în baza unui contract comercial sau de colaborare.
Regulament de Acces la Reţeaua de Comunicaţii	1. Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către D.C.D. 2. Departamentele şi Facultăţile trebuie să aprobe, în scris, conectarea dispozitivele 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 comunica D.C.D. 3. Conectarea sistemelor de calcul care nu sunt proprietatea Universităţii „Alexandru Ioan Cuza” din Iaşi se face numai cu aprobarea în scris a D.C.D. la recomandarea Departamentelor sau a Facultăţilor. 4. Accesul de la distanţă la reţeaua Universităţii “Alexandru Ioan Cuza” din Iaşi se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (*Internet Service Provider* (ISP)) agreat de către Universitatea “Alexandru Ioan Cuza” din Iaşi şi folosind protocoale aprobate de către D.C.D. 5. Utilizatorii RIC din interiorul Universităţii “Alexandru Ioan Cuza” nu se pot conecta la altă reţea. 6. Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel (pe nici o cale). Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Facultăţilor şi a Departamentelor de către D.C.D. 7. Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea D.C.D. 8. Sistemele computerizate din afara Universităţii care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale Universităţii “Alexandru Ioan Cuza”. 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 Universităţii „Alexandru Ioan Cuza” din Iaşi, nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt

	conectaţi la reţeaua Universităţii. 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 D.C.D. 12. Serviciile de interconectare a reţelei Universităţii “Alexandru Ioan Cuza” Iasi cu alte reţele sunt realizate exclusiv de către D.C.D. 13. Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea D.C.D. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către D.C.D.
Măsuri Disciplinare	Încălcarea acestui regulament se sancţionează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaţilor, 2. Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenţilor, 4. Interzicerea accesului la sistemul RIC, Toate acţiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziţii	Acest Regulament are ca parte integrantă următoarele dispoziţii: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct răspunzător pentru acţiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Utilizarea RIC se face numai în interes de serviciu. 4. Accesul extern la şi de la RIC trebuie să se încadreze în specificaţiile de securitate publicate ale Universităţii „Alexandru Ioan Cuza” din Iaşi. 5. Nu există nici o asigurare a confidenţialităţii datelor personale sau a accesului la informaţii folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe 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. 6. Departamentele şi facultăţile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 7. 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.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru

	asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

6. Configurarea Parametrilor de Acces la Rețea

Introducere	Rețeaua de comunicații a Universității “Alexandru Ioan Cuza” constituie unul din principalele mijloace de exploatare a resurselor informatice. Aceasta include toate echipamentele, cablurile, canalele de cabluri, punctele de acces, punctele de distribuție şi nodurile principale. Este important ca aceasta să se dezvolte controlat şi continuu în condiții de flexibilitate şi evolutivitate. Este important ca dezvoltarea rețelei de comunicații să se facă având în vedere atât cerințele utilizatorilor privind furnizarea de servicii avansate şi diferențiate cât cerințele privind securitatea întregului ansamblu.
Scop	Scopul Regulamentului privind Configurarea Sistemelor pentru Acces la Rețeaua de Comunicații a Universității “Alexandru Ioan Cuza” din Iaşi constă în stabilirea regulilor pentru operarea rețelei de comunicații. Aceste reguli sunt necesare pentru păstrarea integrității, disponibilității şi confidențialității informației din cadrul RIC ale Universitatea “Alexandru Ioan Cuza”.
Audiență	Regulamentul de Acces la Rețeaua de Comunicații a Universității “Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor utilizatorilor care au acces la orice RIC.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iaşi. *Ofițer responsabil cu Securitatea RIC (OSRIC):* Răspunde în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Universității “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universității “Alexandru Ioan Cuza” pentru orice problemă în

	legătură cu securitatea RIC. Funcția OSRIC este asumată de către şeful Departamentului de Comunicații Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcția de OSRIC, persoană care trebuie validată de către ARIC . *Ofițer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății şi validat de către OSRIC. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Furnizor*: Persoană fizică/juridică care oferă bunuri sau servicii Universității “Alexandru Ioan Cuza” din Iaşi în baza unui contract comercial sau de colaborare.
Regulament privind Configurarea Sistemelor Informatice pentru Acces la Rețeaua de Comunicații	1. Infrastructura de comunicații, rețeaua de comunicații digitale, a “Universității Alexandru Ioan Cuza” din Iaşi este administrată de către D.C.D. care este responsabil cu întreținerea şi dezvoltarea acesteia. 2. Pentru a furniza o infrastructură de comunicații unitară cu posibilități de modernizare toate componentele acesteia sunt instalate de către D.C.D. sau de către un furnizor avizat explicit de către D.C.D. 3. Toate echipamentele, fără excepție, conectate la rețeaua de comunicații trebuie configurate conform specificațiilor D.C.D. 4. Orice dispozitiv hardware, inclusiv plăcile de rețea şi aparatele telefonice, care se va conecta la rețeaua Universității “Alexandru Ioan Cuza” din Iaşi, trebuie să fie însoțit de o aprobare de tip (producător, model etc.) din partea D.C.D. Lista cu dispozitivele care pot fi conectate la rețeaua de comunicații a Universității va fi publicată pe sit-ul web al D.C.D. 5. Modificarea configurației oricărui dispozitiv activ conectat la rețeaua de comunicații (inclusiv telefoane) se face numai cu aprobarea D.C.D. 6. Infrastructura de comunicații de date a Universității “Alexandru Ioan Cuza” suportă un set definit de protocoale de rețea (TCP/IP). Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către D.C.D. 7. Infrastructura de comunicații telefonice a Universității “Alexandru Ioan Cuza” suportă un set definit de protocoale (DTMF cu detecție automata în centrală) 8. Adresele de rețea sunt alocate dinamic sau static numai de către D.C.D. 9. Numerele de telefon sunt alocate numai de către D.C.D. 10. Toate conectările în rețeaua de comunicații a Universității “Alexandru Ioan Cuza” sunt responsabilitatea D.C.D., conectarea se va face numai în baza unei cereri standard aprobată de către Departament sau Facultate şi de către conducerea Universității. Formularele vor fi puse la dispoziție prin intermediul sit-ului web al D.C.D. 11. Toate conectările dintre rețeaua de comunicații a Universității “Alexandru Ioan Cuza” şi alte rețele de comunicații, publice sau private, sunt responsabilitatea exclusivă a D.C.D. 12. Echipamentele de protecție a rețelei de comunicație a Universității “Alexandru Ioan Cuza” din Iaşi (firewall) se vor instala de către D.C.D.

	13. Utilizarea sistemelor de protecție (firewall) din Departamente şi Facultăți nu este permisă fără autorizație scrisă din partea D.C.D. Această restricție se aplică şi în cazul în care se folosesc adrese private de rețea. 14. Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile rețelei (este interzisă instalarea unui telefon, fax, modem, router, switch, hub sau punct de acces la rețeaua Universității) fără aprobare din partea D.C.D. Utilizatorilor li se interzice instalarea de dispozitive hardware de rețea sau programe care furnizează servicii de rețea fără aprobarea D.C.D. 15. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale rețelei.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integrantă următoarele dispoziții: 1. Rețeaua de comunicații a Universității Alexandru Ioan Cuza Iaşi este permanent monitorizată de către D.C.D. care răspunde de buna funcționare a acesteia. 2. Sistemele şi echipamentele asociate RIC din cadrul Universității “Alexandru Ioan Cuza” din Iaşi utilizate pentru activitățile Universității care sunt dirijate/controlate şi administrate din exteriorul Universității trebuie sa îndeplinească cerințe specifice si vor fi monitorizate de către D.C.D. 3. Accesul extern la şi de la RIC trebuie să se încadreze în specificațiile de securitate ale Universității „Alexandru Ioan Cuza” din Iaşi. 4. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct pentru acțiunile care pot afecta securitatea RIC. 5. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 6. Utilizarea RIC se face numai în interes de serviciu. 7. Accesul extern la şi de la RIC trebuie să se încadreze în specificațiile de securitate publicate ale Universității „Alexandru Ioan Cuza” din Iaşi. 8. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare. 9. Departamentele şi facultățile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 10. Orice informație folosită în sistemul RIC trebuie să fie păstrată

	confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar.
Referințe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

7. Tratarea Incidentelor de Securitate

Introducere	Numărul de incidente legate de securitatea sistemelor de calcul şi de comunicații şi costul rezultat al întreruperilor şi restaurării serviciilor continuă să crească. Implementarea unor regulamente privind securitatea acestor echipamente, blocarea şi filtrarea accesului la resurse în funcție de necesități, conştientizarea aspectelor legate de securitate de către utilizatori, detectarea în timp util a incidentelor de securitate pentru atenuarea efectelor lor sunt câteva măsuri ce pot fi luate pentru a reduce riscul si costul asociate.
Scop	Acest document descrie cerințele şi regulile care trebuie respectate pentru a minimiza impactul incidentelor de securitate. Acestea includ (dar nu sunt limitate la): detectarea programelor de tip virus, vierme informatic etc, folosirea neautorizată a conturilor de acces, şi a calculatoarelor în sine, precum şi reclamațiile privind folosirea improprie a RIC după cum este subliniat în regulamente.
Audiență	Regulamentul privind Tratarea Incidentelor de Securitate se aplică nediscriminatoriu tuturor persoanelor care folosesc orice componentă a RIC.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iaşi. *Ofițer responsabil cu Securitatea RIC (OSRIC):* Răspunde în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Universității “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universității “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcția OSRIC este asumată de către şeful

	Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC . *Ofiţer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăţi. Acesta este desemnat de către conducătorul Departamentului/Facultăţii şi validat de către OSRIC. *Utilizator:* O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Echipă de Răspuns la Incidentele de Securitate a RIC (ERIS*): personalul responsabil de acţiunile desfăşurate în scopul micşorării sau eliminării impactului negativ al unui incident de securitate. *Virus:* Un program care se auto-ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte de la cele deranjante până la cele distructive. Un virus se execută în momentul în care este accesat un fişier infectat. Un virus de macro infectează codul executabil încapsulat în pachetul de programe Microsoft Office (Word, Excel, PowerPoint) sau alte programe care permit utilizatorului să genereze macro-uri. *Vierme*: Un program care se auto-copiază în oricare altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul reţelei. Prima utilizare a termenului descria un program care s-a multiplicat într-o reţea de calculatoare, folosind resursele sau calculatoarele neutilizate din reţea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o ameninţare la adresa securităţii datorită faptului că folosesc reţeaua pentru a se împrăştia, împotriva voinţei proprietarilor de sisteme de calcul, cauzând astfel nefuncţionarea sau funcţionarea defectuoasă a reţelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferenţa constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere pentru a se multiplica. *Cal troian:* de obicei un virus sau un vierme – care este ascuns sub forma unui program atractiv sau inofensiv, cum ar fi un joc, sau program de grafică (o felicitare în format electronic, un program tip screen-saver). Victimele pot primi un astfel de cal troian prin email sau pe o dischetă, adeseori de la o altă victimă necunoscută sau pot fi încurajate să descarce un fişier de pe o pagină Web sau un forum. *Incident de Securitate:* În termeni informatici este definit ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrităţii şi/sau confidenţialităţii informaţiei de pe un sistem informatic automatizat. Aceasta include examinarea sau navigarea neautorizată, întreruperea sau anularea unui serviciu, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea informaţiilor, modificarea informaţiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştiinţa sau intenţia utilizatorului.
Regulament de Tratare a Incidentelor de Securitate	1. Membrii Echipei de Răspuns la Incidentele de Securitate (Membrii ERIS) ai Universităţii “Alexandru Ioan Cuza” din Iaşi, au funcţii şi responsabilităţi pre-definite care pot fi prioritare îndatoririlor obişnuite. 2. 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. 3. OSRIC este responsabil cu înştiințarea şi coordonarea echipei ERIS pentru tratarea incidentului. 4. OSRIC este responsabil cu strângerea dovezilor fizice şi electronice ce vor face parte din documentația pentru tratarea incidentului. 5. Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităților acolo unde este cazul. 6. OSRIC, în colaborare cu ARIC va stabili conținutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informații. 7. OSRIC şi ERIS trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informațiile utile pentru eliminarea sau diminuarea vulnerabilităților care au cauzat incidentul. 8. OSRIC este responsabil cu documentarea anchetei privind incidentul cu asistentă din partea ERIS. 9. OSRIC este responsabil de coordonarea activităților de comunicare cu terți pentru rezolvarea incidentului. 10. În cazul în care incidentul nu implică acțiuni contrare legilor în vigoare OSRIC va recomanda ARIC sancțiuni disciplinare. 11. În cazul în care incidentul implică aplicarea legilor civile sau penale OSRIC va recomanda ARIC sesizarea organelor în drept ale statului şi va acționa ca ofițer de legătură cu acestea.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integrantă următoarele dispoziții: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct răspunzător pentru acțiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Departamentele şi Facultățile vor acorda prioritate activităților ERIS şi vor respecta întocmai toate recomandările şi cerințele membrilor acesteia. 4. Departamentele şi Facultățile trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării RIC pentru protejarea datelor şi programelor împotriva întrebuințării greşite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător. 5. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor

	instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare. 6. Departamentele şi facultățile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 7. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar. 8. Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația şi datele trebuie protejate fiind proprietatea Universității. 9. Orice program comercial utilizat în cadrul RIC trebuie să fie însoțit de Licență care să specifice clar drepturile de utilizare şi restricțiile produsului. Personalul trebuie să respecte prevederile Licențelor si nu este permisă copierea sau distribuirea ilegală a softul cu licența. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăților, îşi rezervă dreptul de a şterge orice produs fără Licență de pe orice sistem din cadrul RIC. 10. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăților, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fişiere: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), pop email, fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip *freeware* şi *shareware*.
Referințe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.

	11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

8. Monitorizarea Resurselor Informatice şi de Comunicații

Introducere	Monitorizarea RIC pentru asigurarea securității sistemului este o metodă utilizată pentru a confirma funcționalitatea şi eficiența măsurilor de securitate. Această activitate constă în următoarele (fără a se limita numai la aceste exemple): • Detectarea automată a intruşilor prin intermediul sistemelor de înregistrare (logare). • Jurnale Firewall • Jurnale ale activității conturilor utilizator • Jurnale ale scanărilor rețea • Jurnale ale aplicațiilor • Jurnale ale solicitărilor de suport tehnic • Jurnale ale erorilor din sisteme şi servere.
Scop	Scopul Regulamentului de Monitorizare a RIC este stabilirea regulilor şi procedurilor pentru verificarea funcționalității şi eficienței măsurilor de securitate. De asemenea această activitate urmăreşte detectarea situațiilor de evitare sau dezactivare a controalelor. Unul din beneficiile monitorizării securității este identificarea din timp a tentativelor de fraudă sau a infracțiunilor şi a vulnerabilităților sistemelor componente ale RIC. Alte beneficii includ: rezolvarea reclamațiilor, monitorizarea serviciilor, estimarea performanțelor sistemelor în vederea întocmirii planurilor de modernizare, etc.
Audiență	Regulamentul de Monitorizare a RIC al Universității „Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicații a Universității „Alexandru Ioan Cuza” din Iaşi.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca

	scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universităţii, titlul este atribuit în mod automat Rectorului Universităţii Alexandru Ioan Cuza Iaşi. *Ofiţer responsabil cu Securitatea RIC (OSRIC):* Răspunde în faţa ARIC privind administrarea funcţiilor de securitate a informaţiei în cadrul Universităţii “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universităţii “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcţia OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC . *Ofiţer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăţi. Acesta este desemnat de către conducătorul Departamentului/Facultăţii şi validat de către OSRIC. *Utilizator:* O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Abuz de privilegii*: Orice acţiune întreprinsă în mod voit de un utilizator, care vine in contradicţie cu regulamentele Universităţii “Alexandru Ioan Cuza” si/sau legile in vigoare, inclusiv cazul in care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective. *Reţea locală (LAN)*: O reţea de comunicaţii de date ce este distribuită pe o zonă restrînsă (de regulă la nivelul unui grup de lucru). Reţeaua locală oferă comunicaţii între calculatoare şi periferice la o viteză de transfer mare şi cu puţine erori.
Regulament de Monitorizare a RIC	1. 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: a. Tipul traficului (ex. structura pe protocoale şi servicii) extern şi conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat. b. 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. c. Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare). 2. Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale Universităţii “Alexandru Ioan Cuza” Iasi. În această categorie intră următoarele (fără a ne limita doar la acestea): a. Jurnale ale sistemelor de detectarea automată a intruşilor. b. Jurnale Firewall c. Jurnale ale activităţii conturilor utilizator d. Jurnale ale scanărilor reţea e. Jurnale ale aplicaţiilor

	f. Jurnale ale solicitărilor de suport tehnic g. Jurnale ale erorilor din sisteme şi servere. h. Jurnale ale echipamentelor de telefonie 3. În mod regulat (cel puţin o dată la şase luni) se vor efectua verificări, de către D.C.D. sau personalul autorizat al Departamenetelor sau Facultăţilor pentru detectarea: a. Parolelor utilizator care nu respectă regulamentele b. Echipamentelor de reţea conectate neautorizat c. Serviciilor de reţea neautorizate d. Serverelor de pagini de web neautorizate e. Echipamentelor ce utilizează resurse comune nesecurizate f. Utilizării de modemuri neautorizate g. Licenţelor pentru sistemele de operare şi programele instalate 4. Orice neregulă privind respectarea regulamentelor de securitate va fi raportată OSRIC sau OSRICD în scopul efectuării de investigaţii.
Măsuri Disciplinare	Încălcarea acestui regulament se sancţionează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaţilor, 2. Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenţilor, 4. Interzicerea accesului la sistemul RIC, Toate acţiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziţii	Acest Regulament are ca parte integrantă următoarele dispoziţii: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct răspunzător pentru acţiunile care pot afecta securitatea RIC. 2. Accesul la RIC, schimbarea şi monitorizarea drepturilor de acces la RIC trebuie să fie strict supravegheate. Trebuiesc verificate în mod regulat drepturile de acces, precum şi orice modificare a stării postului cum ar fi: transfer, promovare, retrogradare sau terminarea serviciului. 3. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 4. Utilizarea RIC se face numai în interes de serviciu. 5. Nu există nici o asigurare a confidenţialităţii datelor personale sau a accesului la informaţii folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe 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. 6. Departamentele şi facultăţile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 7. 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. 8. Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele trebuie protejate fiind proprietatea Universităţii. 9. Departamentele şi Facultăţile trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIC în scopul 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. 10. 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 sau distribuirea softul cu licenţa. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din cadrul RIC. 11. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fişiere: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), pop email, fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip freeware şi shareware.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

	12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

9. Securitatea Serverelor

Introducere	Serverele sunt acele sisteme care stochează şi distribuie informația către utilizatorii autorizați. În acest context trebuie asigurată integritatea, confidențialitatea si disponibilitatea datelor prin instalarea şi menținerea acestora intr-o manieră care să prevină accesul neautorizat, utilizarea neautorizată şi întreruperea unor servicii.
Scop	Scopul Regulamentului de Securizare a Severelor din Universitatea “Alexandru Ioan Cuza” din Iaşi este de a prezenta cerințele de instalare a unui nou server si de a menține integritatea securității acestuia şi a aplicațiilor.
Audiență	Regulamentul de Securizare a Severelor al Universității „Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicații a Universității „Alexandru Ioan Cuza” din Iaşi.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iaşi. *Ofițer responsabil cu Securitatea RIC (OSRIC):* Răspunde în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Universității “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universității “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcția OSRIC este asumată de către şeful Departamentului de Comunicații Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcția de OSRIC, persoană care trebuie validată de către ARIC . *Ofițer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):*

	Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății şi validat de către OSRIC. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Server:* Un program de calculator care oferă servicii altor programe aflate pe acelaşi calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe acelaşi calculator mai pot rula şi alte programe de tip client sau server
Regulament de Securizare a Severelor	1. Un server nu trebuie conectat la rețeaua Universității “Alexandru Ioan Cuza” din Iaşi până când nu se afla intr-o stare sigura acreditata de către OSRIC sau, după caz, de către OSRICD. 2. Procedura de securizare a serverelor trebuie să includă obligatoriu următoarele: • Instalarea sistemului de operare dintr-o sursa aprobată • aplicarea patch-urilor furnizare de producător • înlăturarea programelor, a serviciilor sistem şi a driver-lor care nu sunt necesare • setarea/activarea parametrilor de securitate, a protecțiilor pentru fişiere şi activarea jurnalelor de monitorizare • dezactivarea sau schimbarea parolelor conturilor predefinite • securizarea accesului fizic la aceste echipamente 3. D.C.D. 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.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integrantă următoarele dispoziții: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct răspunzător pentru acțiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația şi datele trebuie protejate fiind proprietatea Universității. 4. Departamentele şi Facultățile trebuie să ofere facilități

	corespunzătoare de control al accesului în scopul monitorizării RIC în scopul 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. 5. 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 sau distribuirea ilegală a softului cu licenţa. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din cadrul RIC. 6. Departamentul sau Facultatea care cere autorizarea unei aplicaţii trebuie sa parcurgă o procedura de asigurare a securităţii atât pentru aplicaţie cât şi pentru sistem. Documentaţia aferentă va fi supusă aprobării D.C.D. 7. Pentru a asigura o bună separare a îndatoririlor, responsabilităţile proprietarului nu pot fi delegate unui custode.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor

	clasificate.

10. Crearea şi Utilizarea Copiilor de Siguranță (Backup)

Introducere	Copiile de siguranță (*backup*) sunt necesare pentru a permite recuperarea datelor şi aplicațiilor în cazul unor evenimente cum ar fi: dezastre naturale, defecțiuni ale discurilor de sistem, spionaj, erori de introducere a datelor, erori de funcționare a sistemului, etc.
Scop	Scopul Regulamentului de Back-up al Universității “Alexandru Ioan Cuza” din Iaşi este de a stabili regulile pentru crearea copiilor de siguranță (backup) şi stocarea informațiilor electronice ale Universității “Alexandru Ioan Cuza” din Iaşi.
Audiență	Regulamentul privind Crearea Copiilor de Siguranță (*backup*) al Universității “Alexandru Ioan Cuza” din Iaşi se aplică tuturor persoanelor din cadrul Universității “Alexandru Ioan Cuza” care sunt responsabile cu instalarea şi întreținerea de RIC, persoanelor însărcinate cu securitatea RIC şi deținătorilor de informații.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Copii de Siguranță (backup)*: Copii ale fişierelor şi aplicațiilor făcute pentru a evita pierderea datelor şi pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date. *Stocarea Externă (Offsite)*: Stocarea externă trebuie să se realizeze într-o zonă geografică diferită de campus-ul universitar în care este puțin probabil să se producă efecte de acelaşi tip în cazul unui dezastru. Pe baza unei evaluări a informației pentru care s-au realizat copii de siguranță, mutarea mediilor de backup din clădire şi depozitarea lor într-o altă zonă securizată din campusul Universității “Alexandru Ioan Cuza” din Iaşi poate înlocui stocarea externă. *Furnizor*: Persoană fizică/juridică care oferă bunuri sau servicii Universității “Alexandru Ioan Cuza” din Iaşi în baza unui contract comercial sau de colaborare.
Servicii	D.C.D, administratorul RIC poate avea contracte pentru stocarea copiilor de siguranță (backup) în alte zone. Aceste servicii pot fi extinse, la cerere, către toate Departamentele şi Facultățile din Universitatea “Alexandru Ioan

	Cuza”
Regulament privind Crearea şi Utilizarea Copiilor de Siguranţă	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. Furnizorul care oferă servicii de stocare a copiilor de siguranţă în alte zone pentru Universitatea “Alexandru Ioan Cuza” trebuie să fie acreditat în acest scop de către o autoritate a statului. 4. Procedurile stabilite între Universitatea “Alexandru Ioan Cuza” din Iaşi şi furnizorii de stocare ale copiilor de siguranţă în altă zonă trebuie să fie revizuite cel puţin anual. 5. Verificarea copiilor de siguranţă se va face după o procedură documentată şi revizuită periodic. 6. Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţii stocate sunt recuperabile. 7. Accesul la mediile de *backup* ale Universităţii “Alexandru Ioan Cuza” 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. 8. 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.
Măsuri Disciplinare	Încălcarea acestui regulament se sancţionează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaţilor, 2. Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenţilor, 4. Interzicerea accesului la sistemul RIC, Toate acţiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziţii	Acest Regulament are ca parte integranta următoarele dispoziţii: 1. 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. 2. La încheierea relaţiilor cu instituţia, utilizatorii sunt obligaţi să predea toate bunurile materiale si RIC ale Universităţii “Alexandru Ioan Cuza”

	Toate regulamentele privitoare la RIC rămân în vigoare în acest caz până la predarea completa a bunurilor respective. Mai mult, aceasta regulă rămâne valabilă şi după terminarea relaţiilor dintre angajat si instituţie. 3. Departamentul sau Facultatea care cere şi autorizează utilizarea unei aplicaţii trebuie să se asigure în privinţa integrităţii şi securităţii tuturor programelor şi a tuturor fişierelor create de sau achiziţionate pentru aplicaţii. Pentru separarea clară a sarcinilor, atunci când este cazul, responsabilităţile proprietarului nu pot fi delegate către custode. 4. Integritatea programelor de uz general, a programelor utilitare, a sistemelor de operare, a reţelelor şi respectiv a fişierelor de date sunt responsabilitatea Departamentului sau Facultăţii care le are în administrare. Datele destinate testelor şi cercetării trebuie să fie depersonalizate înainte de a fi oferite spre testare, exceptând cazul în care fiecare persoană implicată în testare are acces autorizat la aceste date. 5. Departamentele şi Facultăţile trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIC în scopul 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. 6. Toate Departamentele şi Facultăţile trebuie să evalueze cu atenţie riscul modificării, dezvăluirii neautorizate sau a pierderii datelor pentru care sunt responsabile şi să se asigure prin folosirea sistemelor de monitorizare că Universitatea “Alexandru Ioan Cuza” din Iaşi este protejată împotriva pagubelor financiare sau de orice altă natură. Departamentele şi Facultăţile trebuie să aibă planuri corespunzătoare de recuperare a informaţiilor de orice tip, proprii sau aflate în custodie, în cazul unui dezastru, concepute în funcţie de riscurile posibile şi necesităţile specifice. 7. Toate contractele, licenţele, închirierile, acordurile de consultanţă sau alte reglementari care au ca obiect echipamente/dispozitive din sistemul RIC vor fi autorizate si semnate de către OSRIC sau OSRICD si trebuie sa conţină clauze aprobate de Oficiul Juridic al Universităţii “Alexandru Ioan Cuza” ce aduc la cunoştinţa furnizorilor informaţiile cu privire la rezervarea drepturilor de proprietate si a drepturilor dobândite de către Universitatea “Alexandru Ioan Cuza” asupra RIC, in concordanţă cu regulamentele privind securitatea sistemului de RIC, inclusiv clauze privind întreţinerea şi înapoierea datelor . 8. Orice sistem şi/sau componentă a RIC sau asociate, utilizate pentru activităţile Universităţii “Alexandru Ioan Cuza” şi care sunt dirijate/controlate din exteriorul instituţiei, trebuie să îndeplinească cerinţele contractuale şi vor fi monitorizate din punctul de vedere al securităţii sistemului RIC de către OSRIC sau OSRICD.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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

	corupției. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

11. Detectarea Tentativelor de Acces Neautorizat

Introducere	Detectarea tentativelor de acces neautorizat are un rol important în implementarea şi aplicarea unui regulament de securitate. Pe măsură ce complexitatea sistemelor informaționale şi de comunicații creşte, sistemele de securitate trebuie să evolueze. Odata cu creşterea numărului de vulnerabilități prin utilizarea sistemelor distribuite este necesar un mecanism de asigurare a securității la nivel de sistem precum şi la nivel de rețea. Sistemele de detectare a accesului neautorizat pot contribui la atingerea acestui scop.
Scop	Detectarea tentativelor de acces neautorizat furnizează două funcții importante pentru protejarea resurselor informatice: *Feedback*: informații referitoare la eficiența componentelor din sistemul de securitate. Dacă nu se detectează tentative sau chiar acces neautorizat în condițiile în care se foloseşte un sistem de detectare se consideră că mecanismele de apărare funcționează. *Trigger*: un mecanism automat care determină când este necesară activarea anumitor măsuri specifice ca răspuns la un incident privind accesul neautorizat.
Audiență	Regulamentul privind Detectarea Tentativelor de Acces Neautorizat în sistemul RIC al Universității “Alexandru Ioan Cuza” din Iaşi, se aplică tuturor persoanelor responsabile de instalarea de noi RIC precum şi persoanelor care răspund de utilizarea RIC existente şi persoanelor însărcinate cu Securitatea RIC.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iaşi.

	Ofițer responsabil cu Securitatea RIC (OSRIC): Răspunde în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Universității “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universității “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcția OSRIC este asumată de către şeful Departamentului de Comunicații Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcția de OSRIC, persoană care trebuie validată de către ARIC. *Ofițer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății şi validat de către OSRIC. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Incident de Securitate:* În termeni informatici, este definit ca un eveniment de încercare de pătrundere, o intrare neautorizată sau un atac asupra informației de pe un sistem automatizat din cadrul RIC. Definiția include examinarea sau navigarea neautorizată, întreruperea sau anularea serviciilor, alterarea sau distrugerea datelor, a mediilor de stocare sau a datelor de iesire, modificarea informațiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştirea, indicațiile sau intenția utilizatorului. *Atac informațional*: O încercare de a trece peste măsurile şi controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului de RIC. Atacatorul poate altera informațiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular şi de eficacitatea contramăsurilor aplicate. *Protecție informațională*: Acțiuni întreprinse în vederea afectării informațiilor şi sistemelor informatice ostile, în timp ce protejează informațiile şi sistemele informatice proprii. *Gazdă (Host):* Un sistem care oferă servicii pentru un anumit număr de utilizatori. *Server:* Un program care oferă servicii altor programe aflate pe acelaşi sistem de calcul sau pe alte sisteme conectate în rețea. Un sistem de calcul care rulează un program de tip server este adesea numit server, cu toate că pe acelaşi calculator mai pot rula şi alte programe de tip client sau server. *Firewall:* Un mecanism de control al accesului care acționează ca o barieră între două sau mai multe segmente ale unei rețele de calculatoare sau ale unei arhitecturi de tip client/server, folosit pentru a proteja rețelele interne sau segmente ale acestora împotriva utilizatorilor sau proceselor neautorizate.
Regulament pentru Detectarea Accesului Neautorizat	1. Procesele de înregistrare şi verificare a activității sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcționale pe toate sistemele active (host, server, echipamente de rețea). 2. Trebuie activate funcțiile de anunțare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la rețea. 3. Trebuie activate funcțiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.

	4. Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către administratorul de sistem. 5. Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip firewall sau dispozitive de control al accesului. 6. Înregistrările de verificare pentru serverele şi host-urile din rețeaua internă trebuie revizuite cel puțin săptămânal. Administratorul de sistem va furniza aceste înregistrări de verificare la cererea OSRIC sau OSRICD. 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 OSRIC. 10. Utilizatorii sunt obligați să raporteze orice anomalii în performanța sistemelor utilizate cât şi orice semne ale unor posibile infracțiuni la OSRIC sau OSRICD.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integranta următoarele dispoziții: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct răspunzător pentru acțiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Controalele de securitate a RIC nu trebuie ocolite sau dezactivate. 4. Utilizarea RIC se face numai în interes de serviciu. 5. Departamentele şi facultățile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 6. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar. 7. Departamentele şi Facultățile trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării RIC în scopul protejării datelor şi programelor împotriva întrebuințării greşite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător.

	8. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fişiere: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), pop email, fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip freeware şi shareware.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.

12. Utilizarea Calculatoarelor Portabile

Introducere	Dispozitivele de calcul portabile (*laptop*, PDA, etc.) devin din ce în ce mai puternice şi accesibile. Dimensiunile acestora şi funcţionalitatea din ce în ce mai complexă fac ca acestea să fie preferate calculatoarele obişnuite. Mobilitatea dispozitivelor informatice şi de comunicaţii poate conduce la probleme specifice privind securitatea informaţiilor.
Scop	Scopul Regulamentului privind Securitatea Informaţiilor în cazul utilizării Calculatoarelor Portabile este de a stabili regulile de folosire şi de conectare a acestora în reţeaua de comunicaţii a Universităţii “Alexandru Ioan Cuza” din Iaşi. Aceste reguli sunt necesare pentru păstrarea integrităţii, disponibilităţii şi confidenţialităţii informaţiilor din sistemul RIC.
Audienţă	Regulamentul privind Securitatea Informaţiilor în cazul utilizării Calculatoarelor Portabile se aplică în mod egal, nediscriminatoriu, tuturor persoanelor ce utilizează calculatoarele portabile şi folosesc RIC ale Universităţii „Alexandru Ioan Cuza” din Iaşi.
Definiţii	*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: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia. *Administratorul Resurselor Informatice si de Comunicaţii (ARIC):* Responsabil la nivelul Universităţii cu administrarea şi finanţarea RIC ale Universităţii „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universităţii, titlul este atribuit în mod automat Rectorului Universităţii Alexandru Ioan Cuza Iaşi. *Ofiţer responsabil cu Securitatea RIC (OSRIC):* Răspunde în faţa ARIC privind administrarea funcţiilor de securitate a informaţiei în cadrul Universităţii “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universităţii “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcţia OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC.

	Ofițer responsabil cu securitatea RIC la nivel Departamental: (OSRICD): Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății şi validat de către OSRIC. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Dispozitive de Calcul Portabile:* Orice dispozitiv uşor de transportat care este capabil să recepționeze şi/sau transmită date la, şi de la RIC. Acestea includ, dar nu se limitează la, calculatoare-agendă (notebook-uri), calculatoare de buzunar, asistenți digitali personali (Personal Digital Assistants - PDAs), pagere, şi telefoane celulare.
Regulamentul privind Securitatea Informațiilor în cazul utilizării Calculatoarelor Portabile	1. Departamentele şi Facultățile trebuie să aprobe, în scris, conectarea dispozitivele portabile la RIC ale Universității. 2. Calculatoarele portabile trebuie să fie protejate prin parole. 3. Se va evita stocarea datelor care privesc Universitatea „Alexandru Ioan Cuza” pe dispozitivele portabile. În cazul în care nu există o altă alternativă de stocare locală, toate datele care privesc Universitatea „Alexandru Ioan Cuza” din Iaşi trebuiesc criptate utilizând tehnici aprobate. 4. Transmiterea datelor prin rețele de tip wireless se poate face numai prin rețelele instalate de către D.C.D.; acestea vor utiliza tehnici de criptare pentru protejarea datelor transmise. 5. Toate accesările de la distanță a RIC trebuie să se efectueze prin intermediul serviciului autorizat conform Regulamentului privind Securitatea Accesului la Rețea. 6. Conectarea sistemelor de calcul care nu sunt proprietatea Universității „Alexandru Ioan Cuza” din Iaşi se face numai cu aprobarea în scris a D.C.D. la recomandarea Departamentelor sau a Facultăților. 7. Dispozitivele portabile de calcul neutilizate trebuie securizate fizic. Aceasta presupune încuierea lor într-un birou, într-un sertar de birou sau cabinet, sau ataşat la un birou sau cabinet printr-un sistem de blocare prin cablu.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integranta următoarele dispoziții: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct răspunzător pentru acțiunile care pot afecta securitatea RIC. 2. Controalele care vizează securitatea sistemului RIC nu trebuie evitate sau dezactivate.

	3. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 4. Utilizarea RIC se face numai în interes de serviciu. 5. Accesul extern la şi de la RIC trebuie să se încadreze în regulamentele de securitate ale Universităţii „Alexandru Ioan Cuza” din Iaşi. 6. Nu există nici o asigurare a confidenţialităţii datelor personale sau a accesului la informaţii folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe 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. 7. Departamentele şi facultăţile sunt responsabile cu autorizarea utilizatorilor pentru folosirea adecvată a RIC. 8. 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. 9. Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele trebuie protejate fiind proprietatea Universităţii. 10. Departamentele şi Facultăţile trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIC în scopul 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. 11. 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 sau distribuirea ilegală a softul cu licenţa. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din cadrul RIC. 12. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fişiere: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), pop email, fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip freeware şi shareware.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.

	5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

13. Modificări şi Modernizări ale Sistemului Resurselor Informatice şi de Comunicații

Introducere	Sistemul RIC din cadrul Universității “Alexandru Ioan Cuza” din Iaşi este în continuă dezvoltare şi extindere. Numărul utilizatorilor creşte continuu odată cu cerințele pentru servicii specifice (mai multe echipamente-client, mai multe aplicații etc.) iar activitatea acestora depinde din ce în ce mai mult de funcționarea rețelei de comunicații. Pe măsură ce interdependențele în infrastructura RIC se dezvoltă, necesitatea unui proces de administrare a modificărilor şi modernizărilor este esențial. La anumite intervale de timp, fiecare element al sistemului RIC trebuie oprit pentru modernizare, întreținere sau configurare. În plus, pot apare întreruperi neplanificate care conduc la operații suplimentare ce afectează funcționarea ansamblului RIC. Modul de tratare a acestor modificări reprezintă o parte critică în procesul de realizare a unei infrastructuri robuste şi utile a RIC.
Scop	Scopul Regulamentului pentru Modificări şi Modernizări ale Sistemului RIC este de a stabili un cadru rațional şi predictibil, astfel încât utilizatorii să-şi poată planifica acțiunile în consecință. Acțiunile de modificare şi modernizare necesită o anticipare a evenimentelor, monitorizare, şi evaluare a performanțelor pentru a reduce impactul negativ asupra comunității de utilizatori şi pentru a îmbunătăți serviciile oferite prin RIC.
Audiență	Regulamentul pentru Modificări şi Modernizări ale Sistemului RIC se aplică tuturor persoanelor care instalează, administrează şi întrețin Resursele Informatice şi de Comunicați.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Modificare*: Orice implementare a unei noi funcționalități (adăugare de servicii/funcții/echipamente), orice întrerupere a unui echipament/serviciu, orice reparație a unui echipament/serviciu existent şi orice mutare sau

	suprimare a unui echipament/serviciu. *Modificare planificată* : Proces de modificare a unui echipament sau serviciu anunțat, documentat, aprobat. *Modificare neplanificată*: Proces de modificare a unui echipament sau serviciu în care nu s-a reuşit anunțarea, documentarea şi aprobarea prealabilă. Aceste modificări vor fi anunțate ulterior şi sunt acceptate doar în situațiile în care există motive întemeiate (ex. defecțiuni). *Modificare urgentă*: Proces de intervenție neautorizată imediată asupra unui echipament cauzată de iminența unui eveniment critic în scopul prevenirii distrugerilor pe arii extinse. *Controlul Modificărilor:* Procesul de control al procedurilor privind modificările hardware, software sau firmware etc, astfel încât să se asigure protejarea RIC împotriva modificărilor necorespunzătoare.
Regulament pentru Modificări şi Modernizări ale RIC	Orice modificare asupra unei componente a RIC din cadrul Universității “Alexandru Ioan Cuza” din Iaşi, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de rețea, aplicații, este supusă prezentului regulament şi trebuie să urmeze procedurile în vigoare. Toate modificările care afectează mediul de funcționare a sistemelor componente ale RIC (ex: aparate de aer condiționat, instalații de apă, încălzire, instalații electrice şi alarme) trebuie să fie anunțate 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 ARIC. 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 Facultății. Orice cerere de modificare planificată trebuie să obțină o aprobare formală din partea Departamentului sau Facultății care administrează resursele supuse modificărilor. Modificările planificate trebuie anunțate cu cel putin 48 ore înainte de a fi executate. Cererile de modificare planificată pot fi respinse în următoarele cazuri, dar nu numai: planificare inadecvată, planuri de refacere a serviciilor inadecvate, durata modificării poate afecta în mod negativ o activitate importantă a instituției, sau resursele corespunzătoare necesare nu pot fi disponibile imediat. 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 întreținută o bază de date care să cuprindă toate modificările. Acesta trebuie să conțină cel puțin următoarele informații: data la care s-a făcut cererea pentru modificare şi data la care s-a făcut modificarea; informații de contact pentru utilizator; natura modificării; indicarea succesului sau nereuşitei modificării.

Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integrantă următoarele dispoziții: 1. Infrastructura sistemului RIC se află sub controlul D.C.D. Trebuie obținută aprobarea din partea D.C.D. înainte de conectarea unui echipament la rețea. D.C.D. îşi rezervă dreptul de a deconecta orice echipament de rețea care nu este conform cu standardele sau care nu este considerat a fi securizat în mod corespunzător . 2. Integritatea programelor de uz general, a programelor utilitare, a sistemelor de operare, a rețelelor şi respectiv a fişierelor de date sunt responsabilitatea Departamentului sau Facultății care deține echipamentul. Datele destinate testelor şi cercetării trebuie să fie de uz general (depersonalizate) înainte de a fi oferite spre testare, exceptând cazul în care fiecare persoană implicată în testare are acces autorizat la aceste date. 3. Toate modificările aduse sistemelor, programelor sau datelor trebuie aprobate de către Departamentul sau Facultatea care deține echipamentele sau este responsabil de integritatea acestora.
Referințe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi

	libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

14. Utilizare Internet şi Intranet

Introducere	În acord cu prevederile din prezentul Regulament, Resursele Informatice şi de Comunicaţii (RIC) sunt bunuri strategice ale Universităţii „Alexandru Ioan Cuza” din Iaşi care trebuie administrate ca resurse ale statului român. Acest regulament este stabilit pentru a atinge următoarele scopuri: 1. Să fie în conformitate cu statutele, regulamentele şi alte documente oficiale în vigoare pentru administrarea resurselor informatice, 2. Să stabilească practici prudente şi acceptabile privind utilizarea reţelei Internet, 3. Să instruiască utilizatorii care pot folosi reţeaua Internet în ceea ce priveşte responsabilităţile lor asociate unei astfel de utilizări.
Audienţă	Regulamentul de Utilizare Internet şi Intranet se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii „Alexandru Ioan Cuza” din Iaşi care are capacitatea de acces Internet şi/sau Intranet.
Definiţii	*Resurse Informatice şi de Comunicaţii (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare, precum şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze e-mail, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia. *Administratorul Resurselor Informatice si de Comunicaţii (ARIC):* Responsabil la nivelul Universităţii cu administrarea şi finanţarea RIC ale Universităţii „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universităţii, titlul este atribuit în mod automat Rectorului Universităţii Alexandru Ioan Cuza Iaşi. *Ofiţer responsabil cu Securitatea RIC (OSRIC):* Răspunde în faţa ARIC privind administrarea funcţiilor de securitate a informaţiei în cadrul Universităţii “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universităţii “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcţia OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC. *Ofiţer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de

	securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăţi. Acesta este desemnat de către conducătorul Departamentului/Facultăţii şi validat de către OSRIC. *Utilizator:* O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Internet:* Sistem global care interconectează calculatoare şi reţele de calculatoare. Acestea sunt deţinute de mai multe organizaţii, agenţii guvernamentale, societăţi, instituţii academice. *Intranet:* Reţea privată destinată comunicaţiilor şi partajării informaţiilor, care, ca şi reţeaua Internet, foloseşte suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizaţi din cadrul unei organizaţii (instituţii). În mod obişnuit, reţeaua Intranet a unei organizaţii este protejată printr-un sistem de protecţie (firewall).
Drept de Proprietate	Informaţia în format electronic, fişierele create, modificate, trimise, primite sau stocate pe dispozitivele conectate la sistemul RIC, aflate sub administrare, sau în custodia şi sub controlul Universităţii „Alexandru Ioan Cuza”, sunt proprietatea Universităţii, în condiţiile legilor în vigoare.
Confidenţialitate	Fişierele electronice create, modificate, trimise, primite sau stocate pe Resurse Informatice proprii, închiriate, administrate sau în custodia şi sub controlul Universităţii „Alexandru Ioan Cuza” din Iaşi, nu sunt confidenţiale şi pot fi accesate de către personalul responsabil cu securitatea RIC, fără înştiinţarea utilizatorului sau a proprietarului sistemelor. Conţinutul unui fişier electronic poate fi accesat de către personalul autorizat în conformitate cu prevederile şi normele de securitate ce se regăsesc în Regulamentul privind Accesul Administrativ.
Regulament de Utilizare reţea Internet şi Intranet	1. Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopuri academice şi de cercetare. 2. Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către D.C.D. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie de către producător. 3. Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore. 4. Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy şi/sau firewall. 5. Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze Regulamentului de Utilizare Acceptabilă a RIC. 6. Orice activitate a utilizatorilor folosind RIC poate fi înregistrată şi ulterior examinată. 7. Conţinutul tuturor sit-urilor web ale Universităţii „Alexandru Ioan Cuza” din Iaşi trebuie să se conformeze Regulamentelor de Utilizare Acceptabilă a RIC şi să folosească numele de domeniu al Universităţii „Alexandru Ioan Cuza” din Iaşi (uaic.ro). 8. Nu se vor publica pe sit-urile web ale Universităţii “Alexandru Ioan Cuza” din Iaşi materiale cu caracter ofensiv sau de hărţuire. 9. Nu se vor publica pe sit-urile web ale Universităţii “Alexandru Ioan Cuza” din Iaşi, materiale publicitare comerciale sau personale.

	10. Nu se vor publica pe sit-urile web ale Universităţii “Alexandru Ioan Cuza” din Iaşi date ale Universităţii “Alexandru Ioan Cuza” din Iaşi fără asigurarea că materialele sunt disponibile numai persoanelor sau grupurilor autorizate. 11. Nu este permisă utilizarea RIC ale Universităţii “Alexandru Ioan Cuza” din Iaşi în scop personal sau pentru solicitări personale ce nu au legătură cu Universitatea „Alexandru Ioan Cuza” din Iaşi. 12. 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 „Alexandru Ioan Cuza” din Iaşi. 13. Orice material confidenţial al Universităţii „Alexandru Ioan Cuza” din Iaşi transmis prin reţeaua Internet trebuie criptat. 14. 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.
Utilizare Ocazională	1. Utilizarea personală ocazională a RIC pentru acces la reţeaua Internet este permisă doar utilizatorilor care au aprobarea Universităţii „Alexandru Ioan Cuza” din Iaşi; acest drept nu se extinde membrilor familiei sau altor persoane. 2. Utilizarea ocazională nu trebuie să aibă ca rezultat costuri directe pentru Universitatea „Alexandru Ioan Cuza” din Iaşi. 3. Utilizarea ocazională nu trebuie să afecteze îndeplinirea sarcinilor de serviciu ale angajatului sau activitatea studenţilor. 4. Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Universităţii „Alexandru Ioan Cuza” din Iaşi, sau punerea acesteia într-o situaţie delicată. 5. Stocarea fişierelor şi documentelor personale pe Resursele Informatice ale Universităţii „Alexandru Ioan Cuza” din Iaşi, trebuie să fie nominală. 6. Toate fişierele şi documentele – inclusiv cele personale – stocate sau transportate prin intermediul RIC sunt proprietatea Universităţii „Alexandru Ioan Cuza” din Iaşi, în condiţiile legilor în vigoare. Acestea pot fi subiectul cererilor de deschidere a raporturilor, şi pot fi accesate în conformitate cu Regulamentul de Acces Administrativ.
Măsuri Disciplinare	Încălcarea acestui regulament se sancţionează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaţilor, 2. Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenţilor, 4. Interzicerea accesului la sistemul RIC, Toate acţiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziţii	Acest Regulament are ca parte integrantă următoarele dispoziţii: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct responsabil pentru acţiunile care pot afecta securitatea RIC.

	2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Utilizarea RIC se face numai în interes de serviciu. 4. Nu există nici o asigurare a confidenţialităţii datelor personale sau a accesului la informaţii folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe 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. 5. Departamentele şi facultăţile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 6. 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. 7. Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele trebuie protejate fiind proprietatea Universităţii „Alexandru Ioan Cuza” din Iaşi. 8. Departamentele şi Facultăţile trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIC pentru protejarea datelor şi programelor împotriva întrebuinţării greşite, în concordanţă cu necesităţile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător. 9. 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. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din cadrul RIC. 10. ARIC, prin intermediul D.C.D., al Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu atribuţiile de serviciu respective. Exemple de astfel de programe sau fişiere: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), pop e-mail, fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip freeware şi shareware.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

	6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

15. Administrarea Conturilor

Introducere	Conturile utilizator sunt mijloacele utilizate pentru a permite accesul la RIC ale Universităţii „Alexandru Ioan Cuza” din Iaşi. Astfel, crearea, modificarea, controlul şi monitorizarea conturilor utilizator sunt operaţiuni foarte importante în cadrul general al asigurării securităţii sistemului RIC.
Scop	Scopul Regulamentului pentru Administrarea Conturilor din Universitatea „Alexandru Ioan Cuza” din Iaşi este: stabilirea de reguli pentru crearea, utilizarea, monitorizarea, controlul şi ştergerea conturilor utilizator.
Audienţă	Regulamentul pentru Administrarea Conturilor al Universităţii “Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor persoanelor care au acces autorizat la sistemul de RIC din cadrul Universităţii “Alexandru Ioan Cuza”.
Definiţii	*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: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia. *Administratorul Resurselor Informatice si de Comunicaţii (ARIC):* Responsabil la nivelul Universităţii cu administrarea şi finanţarea RIC ale Universităţii „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universităţii, titlul este atribuit în mod automat Rectorului Universităţii Alexandru Ioan Cuza Iaşi. *Ofiţer responsabil cu Securitatea RIC (OSRIC):* Răspunde în faţa ARIC privind administrarea funcţiilor de securitate a informaţiei în cadrul Universităţii “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universităţii “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcţia OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC. *Ofiţer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăţi. Acesta este desemnat de către conducătorul Departamentului/Facultăţii şi validat de către OSRIC.

	Utilizator: O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC.
Regulament de Administrare a Conturilor	1. Toate conturile create trebuie să aibă asociată o cerere şi o aprobare corespunzătoare. 2. Toate conturile utilizator se vor crea in formatul Prenume.Nume. 3. Prin contractul de muncă, contractul de şcolarizare şi/sau alte documente toți utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului RIC. 4. Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces. 5. Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat. 6. Toate parolele pentru conturi trebuie sa fie create şi folosite în conformitate cu Regulamentul privind Parolele de Acces. 7. Conturile utilizator ale persoanelor plecate din Universitate pe timp îndelungat (mai mult de 90 de zile) vor fi dezactivate (conturile nu vor mai putea fi accesate). 8. Toate conturile utilizator care nu au fost accesate timp de 30 de zile vor fi dezactivate. După încă 30 zile conturile vor fi şterse dacă nu s-a solicitat accesul la acestea. Administratorii de sisteme sau alt personal autorizat: 1. Sunt responsabili de ştergerea conturilor persoanelor (utilizatorilor) care nu mai lucrează în Universitatea “Alexandru Ioan Cuza” din Iaşi, sau care nu mai au relații cu Universitatea “Alexandru Ioan Cuza” din Iaşi. 2. Trebuie să aibă o documentație de modificare a conturilor utilizator pentru se pune de acord în situații precum schimbări ale numelor de familie, modificări privind contul (numele contului) modificări ale drepturilor de utilizator. 3. Sunt subiectul verificării independente. 4. Trebuie să furnizeze o listă cu toți utilizatorii (listă de conturi) pentru sistemele pe care le administrează, la cererea conducerii autorizate din Universitatea “Alexandru Ioan Cuza”. 5. Trebuie să coopereze cu OSRIC şi OSRICD pentru investigarea problemelor de securitate.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament se completează cu următoarele dispoziții: 1. Controalele de Securitate ale RIC nu trebuie să fie evitate sau dezactivate.

	2. Conştientizarea importanței măsurilor privind securitatea RIC de către utilizatori trebuie să fie permanent subliniată şi actualizată. 3. Toți utilizatorii răspund de modul în care folosesc, individual, RIC şi sunt direct răspunzători de acțiunile legate de securitatea RIC. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 4. Parolele, Numerele de Identificare Personală (PIN), precum şi alte proceduri de securitate a RIC trebuie să fie protejate de fiecare utilizator împotriva utilizării de către alt utilizator sau altă organizație. Nu este permisă divulgarea informațiilor privind contul de acces personal. 5. Accesul la schimbarea şi utilizarea drepturilor asociate unui cont trebuie să fie strict securizat. Trebuiesc revizuite în mod regulat autorizarea accesului la informație (drepturile de acces), precum şi orice modificare a statutului persoanei care deține un cont de acces cum ar fi: transfer, promovare, retrogradare sau terminarea serviciului. 6. Utilizarea conturilor de acces se face numai în interes de serviciu. 7. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare. 8. Departamentele şi facultățile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 9. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță; tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar. 10. La terminarea relațiilor dintre un utilizator şi Universitatea “Alexandru Ioan Cuza” din Iaşi, acesta trebuie sa predea toate RIC. Toate regulile de securitate privind RIC se aplică si rămân în vigoare în eventualitatea încheierii relațiilor cu Universitatea “Alexandru Ioan Cuza” din Iaşi până la finalizarea procedurii de predare. Mai mult decât atât, Regulamentul rămâne valabil şi după încheierea relațiilor de muncă, colaborare etc. 11. Departamentele şi Facultățile trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării RIC în scopul protejării datelor şi programelor împotriva întrebuințării greşite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător. 12. Departamentele şi Facultățile trebuie să evalueze cu atenție riscul modificării, dezvăluirii neautorizate sau a pierderii datelor pentru care sunt responsabile şi să se asigure prin folosirea sistemelor de monitorizare că Universitatea “Alexandru Ioan Cuza” din Iaşi este protejată împotriva pagubelor financiare sau de orice altă natură.
Referințe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm

	3. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

16. Parole de Acces

Introducere	Autentificarea este necesară pentru a controla accesul utilizatorilor la RIC. Controlul accesului este necesar deoarece accesul neautorizat poate duce la prejudicii cauzate de afectarea confidenţialităţii, integrităţii şi disponibilităţii informaţiilor. Acestea pot avea ca efecte pierderi materiale şi morale pentru Universitatea “Alexandru Ioan Cuza” din Iaşi. Autentificarea utilizatorilor se poate realiza folosind diverse metode: conturi şi parole de acces, dispozitive de identificare, caracteristici biologice.
Scop	Regulamentul pentru Parole de Acces al Universităţii “Alexandru Ioan Cuza” din Iaşi stabileşte reguli şi proceduri obligatorii pentru crearea şi modificarea parolelor de acces la RIC.
Audienţă	Regulamentul pentru Parole de Acces al Universităţii „Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii „Alexandru Ioan Cuza” din Iaşi.
Definiţii	*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: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia. *Administratorul Resurselor Informatice si de Comunicaţii (ARIC):* Responsabil la nivelul Universităţii cu administrarea şi finanţarea RIC ale Universităţii „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universităţii, titlul este atribuit în mod automat Rectorului Universităţii Alexandru Ioan Cuza Iaşi. *Ofiţer responsabil cu Securitatea RIC (OSRIC):* Răspunde în faţa ARIC privind administrarea funcţiilor de securitate a informaţiei în cadrul Universităţii “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universităţii “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcţia OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC . *Ofiţer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):*

	Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății şi validat de către OSRIC. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Parolă*: Şir de caractere utilizat, de regulă, pentru identificarea utilizatorului unui cont de acces, în vederea protejării informațiilor asociate contului utilizator. *Parole complexe:* O parolă complexă este un şir de caractere (secvență de caractere, numere şi caractere speciale) care nu poate fi asociată cu informația publică despre contul utilizator, nu este copiată dintr-un dicționar etc.
Regulament pentru Parolele de Acces	1. Toate parolele trebuie să îndeplinească următoarele condiții: • Să fie schimbate de utilizator în mod regulat, cel puțin 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 trebuiesc divulgate nimănui, nici măcar angajaților care răspund de securitatea sistemelor informatice. 2. Dispozitivele de securitate (ex. card Smart) trebuiesc returnate după terminarea relațiilor cu Universitatea “Alexandru Ioan Cuza”. 3. Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat. 4. Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ. 5. Utilizatorii nu pot folosi programe de stocare a parolelor. Se pot face excepții pentru anumite aplicații (precum backup automat) cu aprobarea OSRIC sau OSRICD. Pentru ca o excepție să fie aprobată, trebuie să existe o procedură pentru schimbarea parolelor. 6. Dispozitivele de calcul nu trebuiesc lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă. 7. 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
Reguli pentru Alegerea unei Parole	1. Parolele trebuiesc schimbate la cel puțin 45 de zile. 2. Parolele trebuie să aibă o lungime minimă de 8 caractere 3. Parolele trebuie să conțină litere mici şi mari şi să aibă cel puțin 2 caractere numerice. Caracterele numerice nu trebuie să se afle la

	începutul sau la sfârşitul parolei. Caractere speciale ar trebui incluse în parole acolo unde sistemul permite. Caracterele speciale sunt: (!@#$%^&*_+=?/~`;:,<>|\). 4. Parolele trebuie să respecte următoarele condiții: • Nu trebuie să coincidă sau să fie asemănătoare cu numele dvs. de utilizator (login-ul); • Nu trebuie să coincidă sau să fie asemănătoare numărul dvs. de angajat ; • Nu trebuie să coincidă sau să fie asemănătoare numele dvs.; • Nu trebuie să coincidă sau să fie asemănătoare numele membrilor familiei; • Nu trebuie să coincidă sau să fie asemănătoare cu o eventuală poreclă (*nickname*); • Nu trebuie să coincidă cu codul numeric personal; • Nu trebuie să coincidă cu data naşterii.; • Nu trebuie să coincidă cu numărul de înmatriculare al maşinii; • Nu trebuie să coincidă cu adresa; • Nu trebuie să fie numărul dvs. de telefon; • Nu trebuie să coincidă cu numele oraşului; • Nu trebuie să coincidă cu numele departamentului etc.; • Nu trebuie să coincidă cu nume de străzi; • Nu trebuie să coincidă cu mărci sau modele de maşini; • Nu trebuie să coincidă cu argouri; • Nu trebuie să coincidă cu obscenități; • Nu trebuie să fie termeni tehnici; • Nu trebuie să coincidă cu numele, mascota sau sloganul unei şcoli; • Nu trebuie să coincidă cu informații despre proprietarul contului care sunt cunoscute sau uşor de ghicit (mâncarea, culoarea preferată, sportul preferat etc.); • Nu trebuie să coincidă cu un acronim popular; • Nu trebuie să fie cuvinte din dicționar; • Nu trebuie să fie opusul tuturor celor de mai sus. • Parolele nu trebuie să fie reutilizate pentru o perioadă de un an. • Parolele nu trebuiesc divulgate în nici o situație • Parolele trebuiesc tratate ca informație confidențială.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC, Toate acțiunile care contravin legilor vor fi raportate organelor competente.

Alte Dispoziţii	1. Utilizatorii trebuie să anunţe OSRIC sau OSRICD în cazul în care se observă orice problemă/breşă în sistemul de securitate a RIC din cadrul Universităţii “Alexandru Ioan Cuza” din Iaşi cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare. 2. Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din RIC pentru care nu au autorizaţie sau consimţământ explicit. 3. 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 si/sau informaţii similare utilizate în scopuri de autorizare şi identificare. 4. Departamentele şi facultăţile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 5. 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. 6. Departamentele şi Facultăţile 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.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie

	a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

17. Sistemul de Mesagerie Electronică

Introducere	Acest regulament este stabilit astfel încât: 1. Să fie în conformitate cu regulamentele şi mandatele în vigoare pentru administrarea RIC. 2. Să stabilească practici prudente şi acceptabile privind utilizarea sistemului de mesagerie electronică (poştă electronică). 3. Să instruiască persoanele ce folosesc sistemul de mesagerie electronică privind responsabilitățile asociate folosirii acestui serviciu.
Scop	Scopul Regulamentului privind Sistemul de Mesagerie Electronică al Universității “Alexandru Ioan Cuza” din Iaşi, este de a stabili regulile pentru utilizarea serviciului de poştă electronică din cadrul Universității “Alexandru Ioan Cuza” din Iaşi, privind trimiterea, primirea sau stocarea mesajelor asociate poştei electronice.
Audiență	Regulamentul privind Sistemul de Mesagerie Electronică al Universității „Alexandru Ioan Cuza” din Iaşi, se aplică nediscriminatoriu tuturor persoanelor care au permisiuni de acces la orice resursă informatică din cadrul Universității care are capacitatea de a trimite, primi sau stoca mesaje asociate poştei electronice.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Sistem de Mesagerie Electronică*: orice program care permite ca mesajele în format electronic să fie transmise de la un sistem de calcul la altul. *Mesagerie Electronică*: orice mesaj, imagine, formular, ataşament, date sau orice alt mijloc de comunicație, trimise, primite sau stocate într-un sistem de mesagerie electronică.
Regulament privind Sistemul de Mesagerie Electronică	1. Toți utilizatorii sistemului RIC, fără excepție, vor folosi adrese e-mail din domeniul uaic.ro (toate adresele e-mail vor avea sufixul uaic.ro). 2. Următoarele activități sunt interzise de regulament: • Trimiterea de mesaje cu caracter de intimidare sau hărțuire; • Folosirea sistemului de mesagerie electronică în scopuri personale; • Folosirea sistemului de mesagerie electronică în scopuri politice

	sau pentru campanii politice; • Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate; • Folosirea altei identități decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ. • Folosirea programelor de poştă electronică neautorizate. 3. Următoarele activități sunt interzise deoarece împiedică buna funcționare a comunicațiilor în rețea şi eficiența sistemelor de mesagerie electronică: • Trimiterea sau retrimiterea email-urilor în lanț; • Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituția. • Trimiterea mesajelor de dimensiuni foarte mari; • Trimiterea sau retrimiterea mesajelor ce pot conține viruşi. 4. Toate informațiile şi datele confidențiale ale Universității “Alexandru Ioan Cuza” din Iaşi, transmise către alte rețele externe, trebuie să fie criptate. 5. Toate activitățile utilizatorilor ce implică accesul şi/sau folosirea RIC ale Universității “Alexandru Ioan Cuza” pot fi oricând înregistrate şi analizate. 6. Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că îşi spun opinia sau dau declarații în numele Universității „Alexandru Ioan Cuza”, cu excepția situațiilor în care aceştia sunt autorizați în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declarație explicită prin care utilizatorul specifică faptul că nu reprezintă Universitatea “Alexandru Ioan Cuza”. Un exemplu de declarație simplă este: “părerile exprimate sunt personale, şi nu ale Universității ”Alexandru Ioan Cuza” din Iaşi. 7. Utilizatorii nu trebuie sa trimită, retrimită sau să primească informații confidențiale sau senzitive ce privesc „Universitatea Alexandru Ioan Cuza”, folosind conturi utilizator care nu sunt proprietatea Universității „Alexandru Ioan Cuza”. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, AOL mail), precum şi adrese de email puse la dispoziție de alți Furnizorii de Servicii Internet. 8. Utilizatorii nu trebuie sa trimită, retrimită, primească sau să stocheze informații confidențiale sau nesigure, ce privesc Universitatea „Alexandru Ioan Cuza”, folosind dispozitive de comunicații mobile care nu sunt autorizate de Universitatea „Alexandru Ioan Cuza”. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenți digitali personali, pagere ce permit trimiterea/primirea de informații şi telefoanele mobile.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC,

	Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integrantă următoarele dispoziții: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct răspunzător pentru acțiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Utilizarea RIC se face numai în interes de serviciu. 4. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare. 5. Departamentele şi facultățile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 6. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar. 7. Departamentele şi Facultățile trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării sistemului RIC pentru protejarea datelor şi programelor împotriva întrebuințării greşite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător.
Referințe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.

	10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

18. Detectarea Viruşilor

Introducere	Numărul incidentelor de securitate şi costurile ce rezultă din întreruperea şi restabilirea serviciilor RIC sunt în continuă creştere. Câteva dintre acţiunile care pot fi luate pentru reducerea riscurilor şi scăderea costurilor incidentelor de securitate sunt: implementarea unor reguli severe de securitate, blocarea accesului inutil la RIC, detectarea în timp util şi minimizarea efectelor cauzate de incidente de securitate.
Scop	Scopul Regulamentului de Detectare a Viruşilor din RIC este de a descrie măsuri ce trebuie luate pentru prevenirea, detectarea şi îndepărtarea programelor de tip virus, vierme sau altele asemănătoare.
Audienţă	Regulamentul de Detectare a Viruşilor a Resurselor Informatice şi de Comunicaţii al Universităţii „Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii „Alexandru Ioan Cuza” din Iaşi.
Definiţii	*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: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia. *Administratorul Resurselor Informatice si de Comunicaţii (ARIC):* Responsabil la nivelul Universităţii cu administrarea şi finanţarea RIC ale Universităţii „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universităţii, titlul este atribuit în mod automat Rectorului Universităţii Alexandru Ioan Cuza Iaşi. *Ofiţer responsabil cu Securitatea RIC (OSRIC):* Răspunde în faţa ARIC privind administrarea funcţiilor de securitate a informaţiei în cadrul Universităţii “Alexandru Ioan Cuza”. Este persoana de contact intern şi extern a Universităţii “Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcţia OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC. *Ofiţer responsabil cu securitatea RIC la nivel Departamental: (OSRICD):* Persoana responsabilă de monitorizarea şi implementarea controalelor de

	securitate şi a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății şi validat de către OSRIC. *Utilizator:* O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC. *Virus:* Un program care se auto-ataşează la un fişier executabil sau la o aplicație vulnerabilă şi care generează efecte deranjante sau distructive. Un fişier virus se execută în momentul în care este accesat un fişier infectat. *Vierme:* Un program care se auto-copiază într-o altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul rețelei. Prima utilizare a termenului descria un program care se multiplică într-o rețea de calculatoare, folosind resursele sau calculatoarele neutilizate din rețea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o amenințare la adresa securității din cauză că folosesc resursele RIC pentru a se multiplica, cauzând încărcare suplimentară a rețelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferența constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere sau sectoare pentru a se multiplica. *Cal Troian:* De obicei un program de tip virus sau vierme care este ascuns sub aparența unui program atractiv sau inofensiv. Victimele pot primi un astfel de virus prin email sau prin transfer prin rețea sau de pe un mediu de stocare (dischetă, CD).
Regulament de Detectare a Viruşilor	1. Toate stațiile de lucru de sine stătătoare sau conectate la rețeaua de comunicații a Universității “Alexandru Ioan Cuza”, trebuie să utilizeze programe antivirus aprobate de către OSRIC sau, după caz, de către OSRICD. 2. Programele antivirus nu trebuie dezactivate. 3. Configurația programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului. 4. Frecvența actualizărilor automate a programului antivirus trebuie asigurată de către utilizator. 5. Orice server de fişiere conectat la rețeaua Instituției trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curățirii viruşilor care pot infecta fişierele puse la dispoziție. 6. Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat şi trebuie să respecte regulile de instalare şi utilizare a acestui program. 7. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat OSRIC sau OSRICD.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților, 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenților, 4. Interzicerea accesului la sistemul RIC,

	Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziții	Acest Regulament are ca parte integranta următoarele dispoziții: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct responsabil pentru acțiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Utilizarea RIC se face numai în interes de serviciu. 4. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare. 5. Departamentele şi facultățile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 6. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar. 7. Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația şi datele trebuie protejate fiind proprietatea Universității. 8. Departamentele şi Facultățile trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării RIC în scopul protejării datelor şi programelor împotriva întrebuințării greşite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător. 9. Orice program comercial utilizat în cadrul sistemului RIC trebuie să fie însoțit de Licență care să specifice clar drepturile de utilizare şi restricțiile produsului. Personalul trebuie să respecte prevederile Licențelor si nu este permisă copierea ilegală a softului cu licență. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăților, îşi rezervă dreptul de a şterge orice produs fără Licență de pe orice sistem din cadrul RIC. 10. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăților, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fişiere: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), pop email, fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip freeware şi shareware.
Referințe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.

	4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.

19. Licenţe de utilizare

Introducere	Programele şi tehnologiile informatice sunt protejate prin Licenţe de utilizare. Acestea pot fi utilizate numai în conformitate cu prevederile Licenţelor, prevederi care trebuie cunoscute de către toţi utilizatorii.
Scop	Regulamentul privind Licenţele de Utilizare stabileşte reguli de utilizare a programelor informatice, precum şi a tuturor informaţiilor protejate prin Licenţe în cadrul sistemului RIC al Universităţii “Alexandru Ioan Cuza” din Iaşi.
Audienţă	Regulamentul privind Licenţele de Utilizare al Universităţii „Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii „Alexandru Ioan Cuza” din Iaşi.
Definiţii	*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: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia. *Administratorul Resurselor Informatice si de Comunicaţii (ARIC):* Responsabil la nivelul Universităţii cu administrarea şi finanţarea RIC ale Universităţii “Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universităţii, titlul este atribuit în mod automat Rectorului Universităţii Alexandru Ioan Cuza Iaşi.
Regulament privind Licenţele Programelor	1. Universitatea “Alexandru Ioan Cuza” din Iaşi furnizează un număr suficient de copii cu Licenţă pentru toate programele aprobate spre utilizare astfel încât angajaţii să îşi poată desfăşura munca într-un mod eficient şi rapid. 2. Universitatea “Alexandru Ioan Cuza” din Iaşi trebuie sa se pună de acord în mod adecvat cu furnizorii implicaţi pentru obţinerea de copii adiţionale ale licenţelor dacă şi când acestea sunt necesare în activitatea instituţiei. 3. Copiile suplimentare ale materialelor protejate prin drepturi de autor nu vor fi stocate pe sistemele sau resursele reţelei Universităţii “Alexandru Ioan Cuza” în situaţia în care nu există aprobări specifice. Administratorii de sistem vor şterge produsele şi toate materialele

	protejate prin drepturi de autor în situaţia menţionată, cu excepţia cazului în care utilizatorii implicaţi fac dovada autorizaţiei de folosire sau stocare de la producătorii de drept. 4. Programele sau alte bunuri informatice aflate sub incidenţa drepturilor de autor aflate in posesia Universităţii “Alexandru Ioan Cuza” din Iaşi nu vor fi copiate, cu excepţia cazului în care această copiere este în concordanţă cu prevederile licenţei.
Măsuri Disciplinare	Încălcarea acestui regulament se sancţionează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaţilor, 2. Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenţilor, 4. Interzicerea accesului la sistemul RIC, Toate acţiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziţii	Acest Regulament are ca parte integrantă următoarele dispoziţii: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct responsabil pentru acţiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Utilizarea RIC se face numai în interes de serviciu. 4. Nu există nici o asigurare a confidenţialităţii datelor personale sau a accesului la informaţii folosind protocoale de genul, dar nelimitate la, poştă electronică, navigare pe 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. 5. Departamentele şi facultăţile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 6. 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. 7. 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 sau distribuirea ilegală a softului cu licenţă. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din cadrul RIC. 8. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fişiere: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), pop email, fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip

	freeware şi *shareware*.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.

20. Relații cu Terți

Introducere	Există posibilitatea ca furnizorii, prin condiții stipulate în contracte încheiate cu Universitatea “Alexandru Ioan Cuza”, să necesite acces la sistemul RIC. Exemple de astfel de situații ar putea fi: vizualizare, copiere sau modificare a datelor din jurnale cu informații privind accesul la RIC, instalarea, remedierea sau corectarea programelor sau sistemelor de operare, monitorizarea şi reglarea parametrilor de funcționare ale diverselor dispozitive sau echipamente conectate la sistemul RIC. Stabilirea unor limite şi a unor controale pentru ceea ce poate fi accesat, copiat, modificat şi controlat de către furnizori va elimina sau reduce riscul aducerii de prejudicii materiale sau de natură morală Universității “Alexandru Ioan Cuza” din Iaşi.
Scop	Scopul Regulamentului de Relații cu Terți este de a stabili regulile pentru accesul Furnizorilor la RIC ale Universității “Alexandru Ioan Cuza” şi la serviciile de întreținere (curent, apă, instalații de stingere a incendiilor, instalații de climatizare, instalații de control a accesului etc.) care sunt controlate prin dispozitive ce utilizează sistemul RIC, responsabilitățile ce revin Furnizorului în ceea ce priveşte protecția informației în cadrul Universității “Alexandru Ioan Cuza” din Iaşi.
Audiență	Regulamentul de Relații cu Terți al Universității „Alexandru Ioan Cuza” din Iaşi se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicații a Universității „Alexandru Ioan Cuza” din Iaşi.
Definiții	*Resurse Informatice şi de Comunicații (RIC)*: toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (*notebook*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația. *Administratorul Resurselor Informatice si de Comunicații (ARIC):* Responsabil la nivelul Universității cu administrarea şi finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iaşi. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea şi aprobarea regulamentelor privind activitățile de finanțare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iaşi.

	Furnizor: Persoană fizică/juridică care oferă bunuri sau servicii Universităţii “Alexandru Ioan Cuza” din Iaşi în baza unui contract comercial sau de colaborare.
Regulament de Relaţii cu Terţi	1. Orice activitate desfăşurată de furnizor care implică acces la RIC trebuie să se conformeze cu regulamentele în vigoare ale Universităţii “Alexandru Ioan Cuza” din Iaşi, 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 • Regulamente referitoare la Licenţe • Regulament de Utilizare Acceptabilă 2. În toate convenţiile şi contractele încheiate cu Furnizori trebuie specificate următoarele: • Informaţiile din cadrul Universităţii “Alexandru Ioan Cuza” din Iaşi, 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. 3. Furnizorul trebuie să folosească sistemul RIC din cadrul Universităţii “Alexandru Ioan Cuza” din Iaşi numai în scopul stipulat în contract. 4. Orice altă informaţie din sistemul RIC al Universităţii “Alexandru Ioan Cuza” din Iaşi obţinută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora. 5. Toate echipamentele de întreţinere ale Furnizorului, aflate în reţeaua internă a Universităţii “Alexandru Ioan Cuza” din Iaşi 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 “Alexandru Ioan Cuza” din Iaşi, vor fi scoase din uz la încheierea relaţiilor contractuale. 6. Accesului Furnizorului trebuie să fie identificat în mod unic iar administrarea parolelor sau metodelor de autentificare trebuie să fie în conformitate cu Regulamentul privind Parolele de Acces ale Universităţii “Alexandru Ioan Cuza” şi Regulamentului de Acces Administrativ. 7. 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. 8. 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 “Alexandru Ioan Cuza” din Iaşi sau distruse în cel mult 24 de ore de la producerea evenimentului. 9. În cazul terminării/rezilierii contractului sau la cererea Universităţii

	“Alexandru Ioan Cuza” din Iaşi, 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. 10. În cazul încheierii contractului sau la cererea Universităţii “Alexandru Ioan Cuza” din Iaşi, Furnizorul trebuie să predea imediat toate legitimaţiile, cartelele de acces, echipamentele şi stocurile Universităţii “Alexandru Ioan Cuza” din Iaşi. Echipamentele şi/sau stocurile care urmează a fi reţinute de către Furnizor trebuiesc documentate şi autorizate de Conducerea Universităţii “Alexandru Ioan Cuza”. 11. Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către Universitatea “Alexandru Ioan Cuza” din Iaşi trebuie să fie inventariate corespunzător si să posede drepturi de utilizare atestate prin Licenţe.
Măsuri Disciplinare	Încălcarea acestui regulament se sancţionează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaţilor, 2. Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor; 3. Suspendarea sau exmatricularea în cazul studenţilor, 4. Interzicerea accesului la sistemul RIC, Toate acţiunile care contravin legilor vor fi raportate organelor competente.
Alte Dispoziţii	Acest Regulament are ca parte integrantă următoarele dispoziţii: 1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct răspunzător pentru acţiunile care pot afecta securitatea RIC. 2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament. 3. Utilizarea RIC se face numai în interes de serviciu. 4. Nu există nici o asigurare a confidenţialităţii datelor personale sau a accesului la informaţii folosind protocoale de genul, dar nelimitate la, poştă 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. 5. Departamentele şi facultăţile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC. 6. 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. 7. Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele trebuie protejate fiind proprietatea Universităţii. 8. Departamentele şi Facultăţile trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIC, în scopul 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. 9. 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 sau distribuirea ilegală a softului cu licenţa. ARIC, prin intermediul D.C.D., a Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din cadrul RIC. 10. La încheierea relaţiilor cu Universitatea “Alexandru Ioan Cuza” din Iaşi, utilizatorii sunt obligaţi să predea toate bunurile materiale şi resursele informatice administrate de Universitatea “Alexandru Ioan Cuza”. Toate regulamentele de securitate pentru Resursele Informatice se aplică şi rămân în vigoare în eventualitatea încheierii relaţiilor cu Universitatea “Alexandru Ioan Cuza” până la finalizarea acestei predări. 11. Departamentele şi Facultăţile trebuie să ofere modalităţi corespunzătoare de control al accesului în scopul protejării datelor şi programelor împotriva întrebuinţării greşite. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător. 12. Toate Departamentele şi Facultăţile trebuie să evalueze cu atenţie riscul modificării sau dezvăluirii neautorizate sau a pierderii datelor pentru care sunt responsabile şi să se asigure prin folosirea sistemelor de monitorizare că instituţia (Universitatea “Alexandru Ioan Cuza” din Iaşi) este protejată împotriva pagubelor materiale sau de orice altă natură.
Referinţe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: http://www.iso17799software.com/what.htm 3. Lege 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. 4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 5. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 6. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 7. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public. 8. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică 9. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 10. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 11. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal

	care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date. 12. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu. 13. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.