

	Universitatea „Alexandru Ioan Cuza” Iași	
	Departamentul de Comunicații Digitale	
	Politica de Securitate privind Sistemul Resurselor Informatice și de Comunicații din Universitatea „Alexandru Ioan Cuza”, Iași	

Politica de Securitate privind Sistemul Resurselor Informatice și de Comunicații din Universitatea „Alexandru Ioan Cuza”, Iași

Introducere	<p>În acord cu prevederile din prezentul document, Resursele Informatice și de Comunicații (RIC) sunt bunuri strategice ale Universității „Alexandru Ioan Cuza” din Iași care trebuie administrate ca resurse ale statului român.</p> <p>Compromiterea securității sistemului RIC poate afecta capacitatea Universității „Alexandru Ioan Cuza” din Iași de a oferi servicii informatice și de comunicații, poate conduce la fraude sau distrugerea datelor, violarea clauzelor contractuale, divulgarea secretelor, afectarea credibilității Universității „Alexandru Ioan Cuza” din Iași în fața partenerilor săi.</p> <p>Această politică este stabilită astfel încât:</p> <ul style="list-style-type: none"> • Să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice publice, • Să stabilească practici prudente și acceptabile privind utilizarea RIC ale Universității „Alexandru Ioan Cuza” din Iași, • Să instruiască utilizatorii care au dreptul de folosire a sistemului RIC privind responsabilitățile asociate unei astfel de utilizări.
Audiență	<p>Politica de securitate a sistemului RIC al Universității „Alexandru Ioan Cuza” din Iași se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică și de comunicații a Universității „Alexandru Ioan Cuza” din Iași.</p> <p>Următoarele entități și utilizatori sunt vizați în mod distinct de prevederile Politicii :</p> <ul style="list-style-type: none"> • Angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informațional și de comunicații • Colaboratorii Universității „Alexandru Ioan Cuza” din Iași care au acces la sistemul RIC • Furnizorii Universității „Alexandru Ioan Cuza” din Iași care au acces sistemul RIC • Studenții Universității „Alexandru Ioan Cuza” din Iași • Alte persoane, entități sau organizații care au acces la sistemul RIC
Scop	<p>Politica de securitate a sistemului RIC are ca scop asigurarea integrității, confidențialității și disponibilității informației.</p> <p>Confidențialitatea se referă la protecția datelor împotriva accesului</p>

Versiune: 1.0.0 Aprobat: _____._____ Efectiv: _____._____._____	Creat: D.C.D., 25.05.2004, Modificat: 26.05.2004 Aprobat: Senatul Universității „Alexandru Ioan Cuza” din Iași	Pagina 1 din 10
--	--	--------------------

neautorizat. Fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia și sub controlul Universității „Alexandru Ioan Cuza”, sunt proprietatea Universității în condițiile legilor în vigoare. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la sistemul RIC.

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

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

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor și procedurilor de securitate. Acestea sunt obligatorii pentru toți utilizatorii sistemului RIC.

Definiții

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

Administratorul Resurselor Informatice și de Comunicații (ARIC): Responsabil la nivelul Universității cu administrarea și finanțarea RIC ale Universității „Alexandru Ioan Cuza” din Iași. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea și aprobarea regulamentelor privind activitățile de finanțare, administrare și utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea Universității, titlul este atribuit în mod automat Rectorului Universității Alexandru Ioan Cuza Iași.

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 și extern a Universității „Alexandru Ioan Cuza” pentru orice problemă în legătură cu securitatea RIC. Funcția OSRIC este asumată de către șeful Departamentului de Comunicații Digitale (D.C.D.). Șeful D.C.D. poate numi o altă persoană în funcția de OSRIC, persoană care trebuie validată de către ARIC .

Versiune: 1.0.0

Aprobat: _____._____

Efectiv: _____._____

Creat: D.C.D., 25.05.2004, **Modificat:** 26.05.2004
Aprobat: Senatul Universității „Alexandru Ioan Cuza” din Iași

Pagina
2 din 10

	<p>Ofițer responsabil cu securitatea RIC la nivel Departamental: (OSRICD): Persoana responsabilă de monitorizarea și implementarea controalelor de securitate și a procedurilor pentru sistemul RIC la nivelul unui Departament sau al unei Facultăți. Acesta este desemnat de către conducătorul Departamentului/Facultății și validat de către OSRIC.</p> <p>Utilizator: O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea „Alexandru Ioan Cuza”, în conformitate cu procedurile și regulamentele în vigoare, să folosească RIC.</p> <p>Abuz de privilegii: Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Universității “Alexandru Ioan Cuza” și/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acțiunii respective.</p> <p>Furnizor: Persoană fizică/juridică care oferă bunuri sau servicii Universității “Alexandru Ioan Cuza” din Iași în baza unui contract comercial sau de colaborare.</p>	
Clasificarea Informațiilor	<p>Clasificarea informațiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora cât și pentru a determina pierderile potențiale ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora</p> <p>Pentru a asigura securitatea și integritatea informațiilor, acestea se împart în trei categorii principale:</p> <ul style="list-style-type: none">• <i>Publice</i>• <i>Secrete</i>• <i>Strict Secrete</i> <p>OSRIC, OSRICD și conducerea Facultăților/Departamentelor răspund de evaluarea periodică a schemei de clasificare a informațiilor. Toate informațiile din Universitatea “Alexandru Ioan Cuza” din Iași trebuie să se regăsească în una din următoarele categorii:</p> <ol style="list-style-type: none">1. Publice. Acestea sunt informațiile accesibile oricărui utilizator din interiorul sau exteriorul Universității “Alexandru Ioan Cuza” din Iași. Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra Universității “Alexandru Ioan Cuza” din Iași sau aceste efecte sunt ne semnificative. Utilizatorii care furnizează aceste informații sunt responsabili de asigurarea integrității și disponibilității acestora în raport cu cerințele Universității “Alexandru Ioan Cuza” din Iași. <i>Exemple:</i> Informațiile de pe aviziere, servere web publice, știrile de presă, informările Rectorului.2. Secrete. În această categorie se includ informațiile care datorită valorii economice nu trebuie făcute publice. Se includ aici și informațiile pe care Universitatea “Alexandru Ioan Cuza” din Iași trebuie să le protejeze conform legislației în vigoare. Datorită valorii economice asociate, aceste date trebuie	
Versiune: 1.0.0 Aprobat: _____. Efectiv: _____. _____	Creat: D.C.D., 25.05.2004, Modificat: 26.05.2004 Aprobat: Senatul Universității „Alexandru Ioan Cuza” din Iași	Pagina 3 din 10

	<p>distruse dacă au fost făcute publice. Aceste date vor fi copiate și distribuite în cadrul Universitatea “Alexandru Ioan Cuza” din Iasi doar utilizatorilor autorizați. Distribuirea acestor informații de către utilizatorii autorizați trebuie să se facă pe baza unei clauze de confidențialitate.</p> <p><i>Exemple:</i> clauze contractuale, codul sursă al aplicațiilor.</p> <p>3. Strict Secrete sau Confidențiale. În această categorie se includ toate informațiile care datorită valorii economice nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidența Codului Civil, Penal sau legislației fiscale. Accesul la aceste informații va fi restricționat. Datele strict secrete nu pot fi copiate, distribuite sau șterse fără acordul scris al conducerii Universității.</p> <p><i>Exemple:</i> cheile criptografice.</p>	
Atribuții și Responsabilități	<p>Atribuțiile manageriale includ :</p> <ul style="list-style-type: none">• Orice angajat sau compartiment al Universității „Alexandru Ioan Cuza” din Iași trebuie să se asigure că managementul respectă prevederile prezentei Politici și a regulamentelor sau procedurilor asociate• Administratorii de rețea/sistem/baze de date trebuie să asigure existența jurnalelor și a traseelor auditării pentru orice tip de acces în sistem conform regulamentelor sau procedurilor asociate• Administratorii de rețea/sistem/baze de date trebuie să asigure activarea tuturor mecanismelor de securitate• Compartimentul de audit intern este responsabil de evaluarea schemei de clasificarea a informațiilor. <p>Atribuțiile OSRIC și OSRICD includ:</p> <ul style="list-style-type: none">• Elaborează și propune modificări ale politicii de securitate a sistemului RIC• Elaborează și propune pentru aprobare regulamentele și procedurile de securitate a sistemului RIC în conformitate cu politica de securitate a sistemului RIC• Elaborează proceduri pentru identificarea utilizatorilor sistemului RIC• Tratarea incidentelor de securitate în scopul minimizării efectului distructiv al acestora asupra sistemului RIC• Facilitarea evaluărilor legale, a cerințelor de tip „cele mai bune practici” pe măsură ce aceste devin recunoscute. <p>Atribuții ale utilizatorilor:</p> <ul style="list-style-type: none">• Să cunoască și să respecte prevederile Politicii de Securitate a Sistemului RIC• Să cunoască și să respecte prevederile tuturor Regulamentelor și/sau Procedurile privind securitatea sistemului RIC	
Versiune: 1.0.0 Aprobat: _____. Efectiv: _____._____	Creat: D.C.D., 25.05.2004, Modificat: 26.05.2004 Aprobat: Senatul Universității „Alexandru Ioan Cuza” din Iași	Pagina 4 din 10

	<ul style="list-style-type: none">• Să răspundă direct de securitatea și conținutul informațiilor și resursele informatice și de comunicații încredințate direct sau indirect. <p>Alte atribuții:</p> <ul style="list-style-type: none">• Toți partenerii Universității „Alexandru Ioan Cuza” din Iași (furnizori, agenți, colaboratori etc.) trebuie să accepte și să respecte prezentul document și regulamentele specifice privind sistemul RIC.
--	---

Confidențialitate	<ol style="list-style-type: none">1. Fișierele electronice create, trimise, primite sau stocate folosind sistemul RIC propriu, administrate sau în custodia și sub controlul Universității „Alexandru Ioan Cuza” nu au caracter personal și pot fi accesate oricând de către angajații autorizați din cadrul D.C.D., Departamente și Facultăți fără înștiințarea utilizatorului conform Planului de Securitate.2. În scopul administrării RIC și pentru asigurarea securității RIC personalul autorizat poate revizui sau utiliza orice informație stocată pe sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor (de exemplu, 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 Universității „Alexandru Ioan Cuza”, orice incident de posibilă întrebuițare greșită sau încălcare a acestui regulament (prin contactarea OSRIC sau OSRICD).4. Un mare număr de utilizatori (inclusiv studenți), pot accesa informații din exteriorul sistemului de comunicații al Universității „Alexandru Ioan Cuza” din Iași. În aceste condiții este obligatorie păstrarea confidențialității informațiilor transmise din exteriorul RIC și a informațiilor obținute din interior.5. Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele Universității „Alexandru Ioan Cuza” din Iași pentru care nu au autorizație sau consimțământ explicit.6. Nici un utilizator al sistemului RIC ale Universității „Alexandru Ioan Cuza” din Iași nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemului RIC. Această regulă se extinde și după ce utilizatorul a încheiat relațiile cu Universitatea „Alexandru Ioan Cuza” din Iași.7. Confidențialitatea informațiilor transmise prin intermediul resurselor de comunicații ale terților nu poate fi asigurată. Pentru aceste situații, confidențialitatea și integritatea informațiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligați să se asigure că toate informațiile confidențiale ale Universității „Alexandru Ioan Cuza” din Iași se transmit în așa fel încât să se asigure confidențialitatea și
--------------------------	--

Versiune: 1.0.0

Aprobat: _____._____

Efectiv: _____._____

Creat: D.C.D., 25.05.2004, **Modificat:** 26.05.2004
Aprobat: Senatul Universității „Alexandru Ioan Cuza” din Iași

Pagina
5 din 10

	integritatea acestora.	
Reguli de Utilizare Acceptabilă a sistemului RIC	<ol style="list-style-type: none">1. Utilizarea sistemului RIC se face numai în interes de serviciu2. Utilizatorii trebuie să anunțe OSRIC sau OSRICD în cazul în care se observă orice problemă/breșă în sistemul de securitate a RIC din cadrul Universității “Alexandru Ioan Cuza” din Iași cât și orice posibilă întrebuintare greșită sau încălcare a regulamentelor în vigoare.3. Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și de comunicații și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip în cadrul sistemului RIC al Universității „Alexandru Ioan Cuza” din Iași.4. Utilizatorii nu trebuie să încerce să obțină acces la date sau programe din RIC pentru care nu au autorizație sau consimțământ explicit.5. Utilizatorii nu trebuie să divulge nimănui numerele de acces Dialup sau Dialback prin modem.6. Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive și/sau informații similare utilizate în scopuri de autorizare și identificare.7. Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).8. 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 Iași. Această listă va fi întocmită de către Departamente și Facultăți, aprobată de către OSRIC și publicată de către Departamente și Facultăți.9. Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane; să degradeze performanțele RIC; să împiedice accesul unui utilizator autorizat la RIC; să obțină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente.10. Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității RIC. De exemplu, utilizatorii Universității „Alexandru Ioan Cuza” nu trebuie să ruleze programe de decriptare a parolilor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.11. RIC ale Universității “Alexandru Ioan Cuza” din Iași. nu	
Versiune: 1.0.0 Aprobat: _____. Efectiv: _____. _____	Creat: D.C.D., 25.05.2004, Modificat: 26.05.2004 Aprobat: Senatul Universității „Alexandru Ioan Cuza” din Iași	Pagina 6 din 10

	<p>trebuie folosite pentru beneficiul personal.</p> <ol style="list-style-type: none">12. 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 Universității)13. Accesul la rețeaua Internet prin intermediul RIC se supune aceluiași regulamente care se aplică utilizării din interiorul instituției și Regulamentului pentru Utilizare Internet și Intranet. Angajații nu trebuie să permită membrilor familiei sau altor persoane accesul la RIC ale Universității „Alexandru Ioan Cuza Iași”.14. Utilizatorii care au acces la sistemul RIC al Universității „Alexandru Ioan Cuza” din Iași au obligația de a purta acte și sau legitimații care să ateste calitatea de utilizator autorizat în spațiile Universității „Alexandru Ioan Cuza” din Iași.15. Utilizatorii vor folosi, exclusiv, numele de domeniu (uaic.ro) în toate activitățile desfășurate prin intermediul sau folosind sistemul RIC al Universității „Alexandru Ioan Cuza”. Utilizarea denumirilor pentru calculatoare și a adreselor de e-mail care nu au sufixul uaic.ro este strict interzisă.16. Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor Universității „Alexandru Ioan Cuza” din Iași folosind RIC.	
Reguli de Utilizare Ocazională a Sistemului RIC	<p>În anumite situații, cu permisiunea explicită a OSRIC sau OSRICD, precum și a conducerii Facultăților și/sau Departamentelor este permisă utilizarea ocazională a RIC. În aceste situații se aplică următoarele restricții:</p> <ol style="list-style-type: none">1. Utilizarea personală ocazională a serviciilor de poștă electronică, acces internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricționată la utilizatorii autorizați și nu poate fi extinsă la membrii familiilor sau alte persoane.2. Utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru Universitatea Alexandru Ioan Cuza Iași.3. Utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaților.4. Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Universității Alexandru Ioan Cuza Iași sau prejudicierea, indiferent de formă, a intereselor Universității.5. Stocarea mesajelor de email, a mesajelor de voce, a documentelor și fișierelor personale din cadrul RIC trebuie să fie nominală.6. Toate mesajele, fișierele și documentele – incluzând mesajele personale, fișierele și documentele – localizate în cadrul RIC sunt proprietatea Universității și pot fi subiectul unor cereri de	
Versiune: 1.0.0 Aprobat: _____._____._____ Efectiv: _____._____._____	Creat: D.C.D., 25.05.2004, Modificat: 26.05.2004 Aprobat: Senatul Universității „Alexandru Ioan Cuza” din Iași	Pagina 7 din 10

	verificare/inspectare/accesare conform regulamentelor.	
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: <ol style="list-style-type: none">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: <ol style="list-style-type: none">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. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nu numai, mesagerie electronică, navigare Web, conversații telefonice, transmisie fax-uri și alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare.4. Departamentele și facultățile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC.5. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială și în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale și în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar.6. Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația și datele trebuie protejate fiind proprietatea Universității.7. Departamentele și Facultățile trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării RIC, protejării datelor și programelor împotriva întrebuirii greșite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat și controlat în mod corespunzător.8. Orice program comercial utilizat în cadrul RIC trebuie să fie însoțit de Licență care să specifice clar drepturile de utilizare și restricțiile produsului. Personalul trebuie să respecte prevederile Licențelor și nu este permisă copierea ilegală a programelor comerciale. ARIC, prin intermediul D.C.D., a	
Versiune: 1.0.0 Aprobat: _____. Efectiv: _____. _____	Creat: D.C.D., 25.05.2004, Modificat: 26.05.2004 Aprobat: Senatul Universității „Alexandru Ioan Cuza” din Iași	Pagina 8 din 10

	<p>Departamentelor și Facultăților, își rezervă dreptul de a șterge orice produs fără Licență de pe orice sistem din cadrul RIC.</p> <p>9. ARIC, prin intermediul D.C.D., a Departamentelor și Facultăților, își rezervă dreptul de a șterge, de pe orice sistem, orice program sau fișier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fișiere, dar nu limitate la: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), fișiere cu muzică (mp3, wav etc.), fișiere grafice (bmp, gif, jpg etc.), programe tip <i>freeware</i> și <i>shareware</i>.</p>
Dispoziții Finale	<ol style="list-style-type: none">1. Politica de Securitate a Universității „Alexandru Ioan Cuza” din Iași impune dezvoltarea, gestionarea și punerea în practică de proceduri și/sau regulamente specifice. Toate procedurile și/sau regulamentele de securitate a sistemului RIC fac parte din Planul de Securitate și sunt obligatorii pentru toți utilizatorii.2. OSRIC are obligația de a revizui periodic prezenta Politică de Securitate și a propune dezvoltarea, modificarea Planului de Securitate3. Prevederile Politicii de Securitate vor fi incluse în contractul de munca, contractul de școlarizare cu studenții și toate contractele cu terți (dacă activitatea acestora are legătură cu sistemul Informatic și de Comunicații al Universității)4. Componentele Planului de Securitate vor fi elaborate de către Departamentul de Comunicații Digitale și vor fi propuse pentru aprobare conducerii Universității “Alexandru Ioan Cuza” din Iași.5. Prezentul document și componentele Planului de Securitate vor conține informații de identificare proprii și se va specifica data la care acestea au fost aprobate și data de la care intră în vigoare.6. Prezentul document și Planul de Securitate a sistemului Resurselor Informatice și de Comunicații vor fi disponibile în format electronic pe sit-ul web al Universității “Alexandru Ioan Cuza” din Iași și pe sit-ul web al Departamentului de Comunicații Digitale. Se recomandă ca aceste documente să fie disponibile sau să se facă trimitere la acestea de pe toate sit-urile web din cadrul Universității “Alexandru Ioan Cuza” din Iași7. Modificarea prevederilor unui Regulament/Procedură se face cu aprobarea conducerii Universității „Alexandru Ioan Cuza” din Iași. Fiecare modificare a conținutului va conduce la modificarea versiunii documentului și a informațiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune intră în vigoare.8. Planul de securitate va conține o listă a tuturor regulamentelor/procedurilor aplicabile în sistemul Resurselor Informatice și de Comunicații.

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 și în mediul de afaceri, prevenirea și sancționarea corupției.
4. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal și 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 și 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 și 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 și 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 și 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.

Versiune: 1.0.0

Aprobat: _____._____

Efectiv: _____._____

Creat: D.C.D., 25.05.2004, **Modificat:** 26.05.2004
Aprobat: Senatul Universității „Alexandru Ioan Cuza” din Iași

Pagina
10 din 10