ROMÂNIA
MINISTERUL EDUCAŢIEI NAȚIONALE
UNIVERSITATEA DIN ORADEA

Adresa: C.P. nr.114, Oficiul Poştal Oradea 1,Str. Universităţii nr. 1, Oradea, România
Telef: +40 0259 / 432830 +40 0259 / 408 190, Fax: +40 0259/ 432789
E-mail: rectorat@uoradea.ro, Pagina web: www.uoradea.ro

Politica de securitate a Universităţii din Oradea

AVIZAT	APROBAT
Consiliul de Administraţie (CA)	**Senatul Universităţii din Oradea (SUO)**
Hotărîrea CA nr. 27	Hotărîrea SUO nr.29
Data: 20.05.2013	Data:17.06.2013

Politica de securitate a Universităţii din Oradea

1. Introducere

În acord cu prevederile din prezentul document, Resursele Informatice şi de Comunicaţii (RIC) puse la dispozitie şi administrate de Serviciul Management Integrat IT (SMIIT) sunt bunuri strategice ale Universităţii din Oradea care trebuie administrate ca resurse ale statului român.

Compromiterea securităţii acestor resurse poate afecta capacitatea Universităţii din Oradea de a oferi servicii informatice şi de comunicaţii, poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilităţii instituţiei în faţa partenerilor săi. Această politică este stabilită astfel încât:

- Să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice publice,
- Să stabilească practici prudente şi acceptabile privind utilizarea RIC ale Universităţii din Oradea
- Să instruiască utilizatorii care au dreptul de folosire a RIC privind responsabilităţile asociate unei astfel de utilizări.

2. Audienţă

Politica de securitate a RIC ale Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a instituţiei.

Următoarele entităţi şi utilizatori sunt vizaţi în mod distinct de prevederile Politicii:

- Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- Colaboratorii Universităţii din Oradea care au acces la RIC;
- Furnizorii Universităţii din Oradea care au acces la RIC;
- Studenţii Universităţii din Oradea;
- Alte persoane, entităţi sau organizaţii care au acces la RIC.

3. Scop

Politica de securitate a RIC are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei.

- Confidenţialitatea se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate folosind sistemul RIC proprii, administrate sau în custodia şi sub controlul Universităţii din Oradea sunt confidenţiale şi pot fi accesate de către angajaţii autorizaţi din cadrul Serviciului Management Integrat IT, Departamente / Departamente şi Facultăţi numai în condiţiile prevăzute de lege.
- Integritatea se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate.

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

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

4. 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: mainframeuri, servere, calculatoare personale, calculatoare-agendă (*notebookuri*, *laptop*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), 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.
- *Inginerul de sistem/Administratorul de reţea este şi Administratorul Resurselor Informatice si de Comunicare* (ARIC): Responsabil la nivelul instituţiei cu administrarea RIC ale Universităţii din Oradea.
- *Utilizator*: O persoană, o aplicaţie automatizată sau process utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicaţii.
- *Abuz de privilegii:* Orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele Universităţii din Oradea şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.
- *Furnizor*: Persoană fizică/juridică care oferă bunuri sau servicii Universităţii din Oradea în baza unui contract comercial sau de colaborare.

5. Clasificarea Informaţiilor

Clasificarea informaţiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora cât şi pentru a determina pierderile potenţiale ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.

Pentru a asigura securitatea şi integritatea informaţiilor, acestea se împart în trei categorii principale:

- Publice
- Secrete
- Strict Secrete

Serviciul Management Integrat IT şi conducerea Facultăţilor / Departamentelor / Centrelor răspund de evaluarea periodică a schemei de clasificare a informaţiilor. Toate informaţiile din Universitatea din Oradea trebuie să se regăsească în una din următoarele categorii:

1. **Publice**: Acestea sunt informaţiile accesibile oricărui utilizator din interiorul sau exteriorul Universităţii din Oradea.

Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra instituţiei sau aceste efecte sunt nesemnificative.

Utilizatorii care furnizează aceste informaţii sunt responsabili de asigurarea integrităţii şi disponibilităţii acestora în raport cu cerinţele Universităţii din Oradea.

Exemple: Informaţiile de pe aviziere, servere web publice, ştirile de presă, informările Rectorului sau Senatului.

2. **Secrete**: În această categorie se includ informaţiile care datorită valorii economice nu trebuie făcute publice. Se includ aici şi informaţiile pe care Universitatea din Oradea trebuie să le protejeze conform legislaţiei în vigoare. Datorită valorii economice asociate, aceste date trebuie distruse dacă au fost făcute publice.

   Aceste date vor fi copiate şi distribuite în cadrul Universităţii din Oradea doar utilizatorilor autorizaţi. Distribuirea acestor informaţii de către utilizatorii autorizaţi trebuie să se facă pe baza unei clauze de confidenţialitate.

   Exemple: clauze contractuale, conturi si parole folosite pe serverele de contabilitate sau gestiune a şcolarităţii.

3. **Strict Secrete sau Confidenţiale:** În această categorie se include toate informaţiile care datorită valorii economice nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidenţa Codului Civil, Penal sau legislaţiei fiscale.

   Accesul la aceste informaţii va fi restricţionat. Datele strict secrete nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii Universităţii.

   Exemple: cheile criptografice, conturi administrative de pe serverele de gestiune a şcolarităţii sau de contabilitate.

6. Atribuţii şi Responsabilităţi

Atribuţiile manageriale includ:

- Orice angajat sau compartiment al Universităţii din Oradea trebuie să se asigure că managementul respectă prevederile prezentei Politici şi a regulamentelor sau procedurilor asociate.
- Compartimentul de audit intern este responsabil de evaluarea schemei de clasificare a informaţiilor.
- Administratorii de reţea / sistem / baze de date trebuie să asigure existenţa jurnalelor şi a traseelor auditării pentru orice tip de acces în sistem conform regulamentelor sau procedurilor asociate.
- Administratorii de reţea / sistem / baze de date trebuie să asigure activarea tuturor mecanismelor de securitate.
- Administratorii de reţea / sistem / baze de date elaborează şi propune modificări ale politicii de securitate a sistemului RIC[1].
- Administratorii de reţea / sistem / baze de date elaborează şi propune pentru aprobare regulamentele şi procedurile de securitate a RIC în conformitate cu politica de securitate a acestora[2].
- Administratorii de reţea / sistem / baze de date elaborează proceduri pentru identificarea utilizatorilor RIC[3]
- Administratorii de reţea / sistem / baze de date tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra RIC[4].

[1] Până la înfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)
[2] Până la înfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)
[3] Până la înfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)
[4] Până la înfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

- Administratorii de reţea / sistem / baze de date facilitează evaluările legale, a cerinţelor de tip "cele mai bune practici" pe măsură ce acestea devin recunoscute[5].

Atribuţii ale utilizatorilor:

- Să cunoască şi să respecte prevederile Politicii de Securitate a RIC.
- Să cunoască şi să respecte prevederile tuturor Regulamentelor şi/sau Procedurile privind securitatea RIC.
- Să răspundă direct de securitatea şi conţinutul informaţiilor şi resursele informatice şi de comunicaţii încredinţate direct sau indirect.

Alte atribuţii:

- Toţi partenerii Universităţii din Oradea (furnizori, agenţi, colaboratori etc.) trebuie să accepte şi să respecte prezentul document şi regulamentele specifice privind Resursele Informatice şi de Comunicaţii.

7. Confidenţialitate

1. Fişierele electronice create, trimise, primite sau stocate folosind sistemul RIC proprii, administrate sau în custodia şi sub controlul Universităţii din Oradea sunt confidenţiale şi pot fi accesate de către angajaţii autorizaţi din cadrul Serviciului Management Integrat IT, Departamente / Departamente şi Facultăţi numai în condiţiile prevăzute de lege.
2. În scopul administrării Resurselor Informatice şi de Comunicaţii şi pentru asigurarea securităţii acestora, personalul autorizat poate revizui sau utiliza orice informaţie stocată pe sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor (de exemplu, 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 din Oradea, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea Serviciului Management Integrat IT).
4. Un mare număr de utilizatori (inclusiv studenţi), pot accesa informaţii din exteriorul sistemului de comunicaţii al Universităţii din Oradea. În aceste condiţii este obligatorie păstrarea confidenţialităţii informaţiilor transmise din exteriorul Universităţii din Oradea şi a informaţiilor obţinute din interiorul instituţiei.
5. Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Universitatii din Oradea pentru care nu au autorizaţie sau consimţământ explicit.
6. Nici un utilizator al sistemului RIC a Universităţii din Oradea nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemelor ce compun RIC. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu Universitatea din Oradea.
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 din Oradea se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

[5] Până la înfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

8. Reguli de Utilizare Acceptabilă a Resurselor Informatice şi de Comunicaţii

- Utilizarea RIC se face numai în interes de serviciu.
- Utilizatorii trebuie să anunţe Administratorii de reţea[6] în cazul în care se observă orice problemă / breşă în sistemul de securitate din cadrul Universităţii din Oradea cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.
- Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip în cadrul RIC a Universităţii din Oradea.
- Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din RIC pentru care nu au autorizaţie sau consimţământ explicit.
- Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispositive şi/sau informaţii similare utilizate în scopuri de autorizare şi identificare.
- Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală si a dreptului de autor (*copyright*).
- Utilizatorii nu trebuie să utilizeze programe de tip *shareware* sau *freeware*, fără aprobarea Serviciului Management Integrat IT, cu excepţia cazului în care acestea se găsesc pe lista programelor standard folosite în cadrul Universităţii din Oradea. Această listă va fi întocmită de către Departamente / centre şi Facultăţi, aprobată de către Serviciul Management Integrat IT şi publicată de către Departamente / Centre şi Facultăţi.
- Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane; să degradeze performanţele sistemelor ce alcatuiesc RIC; să împiedice accesul unui utilizator autorizat la RIC; să obţină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente
- Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii sistemelor ce alcatuiesc RIC. De exemplu, utilizatorii Universităţii din Oradea nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente.
- RIC ale Universităţii din Oradea nu trebuiesc folosite pentru beneficiul personal.
- Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Universitatea din Oradea le poate considera ofensive, indecente sau obscene (altele decât cele în curs de cercetare academică unde acest aspect al cercetării are aprobarea explicită a conducerii Universităţii).
- Accesul la reţeaua Internet prin intermediul RIC se supune aceloraşi regulamente care se aplică utilizării din interiorul instituţiei şi Regulamentului pentru Utilizare Internet şi Intranet.
- Angajaţii nu trebuie să permită membrilor familiei sau altor persoane accesul la RIC ale Universităţii.
- Utilizatorii vor folosi, exclusiv, numele de domeniu în toate activităţile desfăşurate prin intermediul sau folosind RIC din Universitatea din Oradea.
- Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor Universităţii din Oradea folosind RIC.
- Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Universităţii din Oradea sau prejudicierea, indiferent de formă, a intereselor Universităţii.
- Fişierele electronice create, trimise, primite sau stocate pe Resurse Informatice proprii, închiriate, administrate sau în custodia şi sub controlul Universităţii din Oradea, cad sub incidenţa

[6] Până la înfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

reglementărilor legale privind proprietatea intelectuală şi pot fi subiectul unor cereri de verificare / inspectare / accesare, conform legislaţiei în vigoare

9. Măsuri Disciplinare

Încălcarea acestui regulament se sancţionează prin măsuri disciplinare care pot include:

- In cazul angajatilor UO, se va proceda la suspendarea accesului la resurse, respectiv la alte masuri disciplinare – conform legislatiei in vigoare
- Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenţilor;
- Interzicerea accesului la Resursele Informatice şi de Comunicaţii.

Toate acţiunile care contravin legilor vor fi raportate organelor competente.

10. 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. 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 electronica poate fi monitorizată în scopul unor investigaţii sau al rezolvării unor plângeri în condiţiile legilor în vigoare.
4. Departamentele/ centrele 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. Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele trebuie protejate.
7. Departamentele / Centrele şi Facultăţile trebuie să ofere facilitate 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.
8. 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. Serviciul Management Integrat IT, direct sau prin intermediul Departamentelor / Centrelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din cadrul RIC.
9. Inginerii de sistem/Administratorii de reţea, direct sau prin intermediul Departamentelor / Centrelor şi Facultăţilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective.

11. Dispoziţii Finale

1. Politica de Securitate a Universităţii din Oradea impune dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau regulamente specifice. Toate procedurile şi/sau regulamentele de securitate a RIC fac parte din Planul de Securitate şi sunt obligatorii pentru toţi utilizatorii.
2. Serviciul Management Integrat IT are obligaţia de a revizui periodic prezenta Politică de Securitate şi a propune dezvoltarea, modificarea Planului de Securitate.
3. În contractele de muncă, contractele de şcolarizare cu studenţii şi contractele cu terţi[7] care implică accesul la resursele sistemului Informatic şi de Comunicaţii al Universităţii, se vor introduce obligatoriu referiri la Regulamentele şi Politica de securitate a RIC.
4. Componentele Planului de Securitate vor fi elaborate de către Serviciul Management Integrat IT şi vor fi propuse pentru aprobare conducerii Universităţii din Oradea.
5. Prezentul document şi componentele Planului de Securitate vor conţine informaţii de identificare proprii şi se va specifica data la care acestea au fost aprobate şi data de la care intră în vigoare.
6. Prezentul document şi Planul de Securitate a sistemului RIC vor fi disponibile în format electronic pe sit-ul web al Universităţii din Oradea şi pe paginile web ale Serviciului Management Integrat IT. Se recomandă ca aceste documente să fie disponibile sau să se facă trimitere la acestea de pe toate sit-urile web din cadrul Universităţii din Oradea.
7. Modificarea prevederilor unui Regulament / Procedură se face cu aprobarea conducerii Universităţii din Oradea. Fiecare modificare a conţinutului va conduce la modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune intră în vigoare.
8. Planul de securitate va conţine o listă a tuturor regulamentelor şi procedurilor aplicabile în sistemul RIC.

12.Referinţe

1. http://dcd.uaic.ro
2. http://www.uaiasi.ro/diacd/
3. http://www.dict.uvt.ro
4. http://www.usamvcluj.ro/CIC
5. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt
6. ISO 17799 – Standard detaliat de securitate:
7. 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.
8. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.
9. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
10. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
11. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
12. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
13. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.

[7] Trebuie să se procedeze in acest sens

15. 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.
16. 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.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.