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

REGULAMENT

de Acces la Reţeaua de Comunicaţii

AVIZAT	APROBAT
Consiliul de Administrație (CA)	**Senatul Universității din Oradea (SUO)**
Hotărîrea CA nr. 27	Hotărîrea SUO nr.
Data: 20.05.2013	Data:

REGULAMENT de Acces la Reţeaua de Comunicaţii

Introducere

Reţeaua de comunicaţii a Universităţii din Oradea constituie unul din principalele mijloace de exploatare a resurselor informatice. Aceasta include toate echipamentele, cablurile, canalele de cabluri, punctele de acces, punctele de distribuţie şi nodurile principale. Este important ca aceasta să se dezvolte controlat şi continuu în condiţii de flexibilitate şi evolutivitate. Este important ca dezvoltarea reţelei de comunicaţii să se facă având în vedere atât cerinţele utilizatorilor privind furnizarea de servicii avansate şi diferenţiate cât şi cerinţele privind securitatea întregului ansamblu.

Scopul

Scopul Regulamentului de Acces la Reţeaua de Comunicaţii a Universităţii din Oradea constă în stabilirea regulilor de acces şi utilizare a acesteia. Aceste reguli sunt necesare pentru păstrarea integrităţii, disponibilităţii şi confidenţialităţii informaţiei din cadrul RIC ale Universităţii din Oradea.

Audienta

Regulamentul de Acces la Reţeaua de Comunicaţii a Universităţii din Oradea se aplică nediscriminatoriu tuturor utilizatorilor care au acces la orice RIC

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), 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.
- *Inginerul de sistem/Administratorul de reţea* îndeplineşte şi funcţia de *Administrator al Resurselor Informatice si de Comunicare* (ARIC)[1], precum şi pe cea de *responsabil cu Securitatea RIC*[2]. Este persoana de contact intern şi extern a Universităţii din Oradea pentru orice problemă în legătură cu securitatea RIC. Directorul SMIIT poate numi o altă persoană în funcţia de responsabil cu probleme de securitate.

[1] Responsabil la nivelul instituţiei cu administrarea RIC ale Universităţii din Oradea
[2] Până la înfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

- *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.

REGULAMENT de Acces la Reţeaua de Comunicaţii

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

2. Departamentele / Centrele şi Facultăţile trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RIC ale Universităţii. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele şi datele de identificare ale acesteia se vor comunica către Serviciul Management Integrat IT[3].

5. Utilizatorii RIC din interiorul Universităţii 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 / Centrelor şi a Departamentelor de către Serviciul Management Integrat IT.

8. Sistemele computerizate din afara Universităţii care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale Universităţii.

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 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 Serviciul de Management Integrat IT.

12. Serviciile de interconectare a reţelei Universităţii cu alte reţele sunt realizate exclusiv de către Serviciul de Management Integrat IT.

13. Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Serviciul de Management Integrat IT.

[3] Trebuie reglementat acest aspect

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.

Referinţe

1. http://dcd.uaic.ro/?page_id=90
2. http://www.uaiasi.ro/diacd/
3. http://www.usamvcluj.ro/CIC/documente/Plan%20de%20securitate.pdf
4. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt
5. ISO 17799 – Standard detaliat de securitate:
6. 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.
7. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.
8. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
9. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
10. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
11. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
12. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.
13. 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.
14. 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.
15. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu.
16. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.