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

privind accesul fizic la Resursele Informatice şi de Comunicaţii

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

REGULAMENT privind accesul fizic la Resursele Informatice şi de Comunicaţii

Introducere

Ca parte a atribuţiilor de serviciu, personalul care asigură suport tehnic, administratorii de reţea, administratorii de sistem sau alte persoane autorizate trebuie să aibă acces la echipamentele şi componentele sistemului *Resurse Informatice şi de Comunicaţii* (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 Serviciul Management Integrat IT şi, acolo unde este cazul, de către fiecare Departament / Centru sau Facultate.

Scopul

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.

Audienta

Regulamentul privind Accesul Fizic la RIC se aplică tuturor persoanelor care răspund de buna funcţionare a infrastructurii, instalarea şi întreţinerea unor componente funcţionale, a personalului responsabil cu securitatea RIC şi utilizatori.

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.
- *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.

REGULAMENT privind accesul fizic la Resursele Informatice şi de Comunicaţii

- Toate sistemele de securitate fizică a Resurselor Informatice şi de Comunicaţii (RIC) – cum ar fi, de exemplu: coduri de acces în clădire şi coduri de acces pentru prevenirea incendiilor - trebuie să fie instalate în conformitate cu regulamentele Universităţii.
- Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat şi monitorizat.
- Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.
- Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RIC se aprobă accesul doar pentru personalul care răspunde de buna funcţionare a echipamentelor din încăperea respectivă şi, dacă este cazul, părţilor contractante, ale căror obligaţii contractuale implică acces fizic.
- Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.
- Acordarea drepturilor de acces (folosind card-uri, chei, parole etc.) se face în scris de către Serviciul Management Integrat IT sau, după caz, Departamentul / Centrul sau Facultatea care deţine încăperea şi resursele.
- Nu este permis transferul dreptului de acces indiferent de motiv.
- Cardurile şi/sau cheile de acces care nu mai sunt folosite trebuie predate Departamentului / Centrului sau Facultăţii care le-a eliberat.
- Pierderea sau furtul cardurilor şi/sau cheilor de acces trebuie raportate imediat Departamentului / Centrului sau Facultăţii care le-a eliberat.
- Cardurile şi/sau cheile nu trebuie să aibă informaţii de identificare, altele decât informaţia de contact necesară pentru returnare.
- Accesul vizitatorilor în spaţiile protejate trebuie documentat pentru fiecare încăpere şi, în cazul în care este permis, se va delega un însoţitor. Vizitatorii trebuie să fie însoţiţi în zonele cu acces restricţionat.
- Fiecare Departament / Centru şi Facultate va ţine o evidenţă a tuturor cardurilor şi/sau cheilor de acces emise, retrase, pierdute sau furate.
- Pentru fiecare spaţiu în care sunt instalate RIC se va păstra o evidenţă a accesului pentru verificări de rutină în situaţii critice.

---

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

- Fiecare Departament / Centru şi/sau Facultate trebuie să verifice periodic drepturile de acces pe bază de card şi/sau cheie şi să anuleze aceste drepturi pentru persoanele care pierd dreptul de acces.
- Fiecare Departament / Centru şi/sau Facultate trebuie să anuleze drepturile de acces ale cardurilor şi/sau cheilor utilizatorilor care îşi schimbă locul de muncă din Universitate sau nu au relaţii contractuale cu Universitatea.
- Pentru fiecare spaţiu cu acces restricţionat trebuie desemnată o persoană care să verifice periodic înregistrările de acces şi să cerceteze orice acces suspect.
- Accesul restricţionat trebuie marcat.

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.

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.