



ROMÂNIA
MINISTERUL EDUCAȚIEI NAȚIONALE
UNIVERSITATEA DIN ORADEA

Adresa: C.P. nr.114, Oficiul Poștal Oradea 1, Str. Universității 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 Administrativ

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

Regulament de Acces Administrativ

Introducere

Personalul care asigură suport tehnic, administratorii de sistem și alte persoane pot avea conturi cu drepturi de acces privilegiat în comparație cu utilizatorii obișnuiți. Datorită faptului că aceste conturi pentru acces administrativ au mai multe privilegii, aprobarea, verificarea și monitorizarea acestora sunt extrem de importante din punctul de vedere al securității RIC.

Scopul

Scopul Regulamentului de Acces Administrativ al Universității din Oradea, este de a stabili regulile pentru crearea, utilizarea, monitorizarea, controlarea și ștergerea conturilor cu drepturi speciale de acces.

Audienta

Procedura de Acces Administrativ se aplică nediscriminatoriu tuturor persoanelor care au sau pot cere și obține drepturi speciale de acces la orice RIC a Universității din Oradea.

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: 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 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.
- *Inginerul de sistem/Administratorul de rețea* îndeplinește și funcția de *Administrator al Resurselor Informatice si de Comunicare (ARIC)*¹, precum și pe cea de *responsabil cu Securitatea RIC*². Este persoana de contact intern și extern a Universității din Oradea pentru orice problemă în legătură cu securitatea RIC. Directorul SMIIT poate numi o altă persoană în funcția de responsabil cu probleme de securitate.
- *Utilizator*: O persoană, o aplicație automatizată sau process utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile și regulamentele în vigoare, să folosească Resursele Informatice și de Comunicații.

¹ Responsabil la nivelul instituției cu administrarea RIC ale Universității din Oradea

² Până la înființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

- *Abuz de privilegii:* Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Universității din Oradea 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.
- *Furnizor:* Persoană fizică/juridică care oferă bunuri sau servicii Universității din Oradea în baza unui contract comercial sau de colaborare.

Regulament de Acces Administrativ

1. Utilizatorii trebuie să cunoască și să accepte toate regulamentele privind securitatea RIC înainte de a li se permite accesul la un cont.
2. Utilizatorii care au conturi de acces administrativ trebuie să aibă instrucțiuni de administrare, documentare, instruire și autorizare a conturilor. Aceste instrucțiuni se vor elabora de către fiecare Departament / Centru sau Facultate și vor fi incluse în fișa postului.
3. Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi și trebuie să facă investigații numai sub îndrumarea Inginerului de sistem/ Administratorului de rețea.
4. Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activității pe care o desfășoară.
5. Accesul administrativ trebuie să se conformeze Regulilor pentru Parolele de acces.
6. Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al Serviciului Management Integrat IT și trebuie să fie schimbată atunci când persoana care utilizează acest cont își schimbă locul de muncă din cadrul Departamentului / Centrului, Facultății sau a Universității, sau în cazul unei modificări a listei de personal ale terților (furnizor desemnat) în contractele cu Universitatea din Oradea.
7. Pentru cazuri de forță majoră accesul cu drept de administrator la resursele RIC ale Universității se va face conform unei proceduri elaborate în acest sens.
8. Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operațiuni definite. Acestea trebuie să îndeplinească următoarele condiții:
 - trebuie să fie autorizate;
 - trebuie create cu dată de expirare specifică;
 - contul va fi șters atunci când nu mai este necesar.

Măsuri Disciplinare

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

- În cazul angajaților UO, se va proceda la suspendarea accesului la resurse, respectiv la alte măsuri disciplinare – conform legislației în vigoare
- Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice și de Comunicații.

Toate acțiunile care contravin legilor vor fi raportate organelor competente.

Referințe

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 transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției.
7. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor.
8. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație 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 informațiile de interes public.
11. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
12. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor 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 protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
14. 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.
15. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
16. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.