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 administrare a conturilor de email

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 de administrare a conturilor de email

Introducere

Conturile utilizator sunt mijloacele utilizate pentru a permite accesul la RIC ale Universităţii din Oradea. Astfel, crearea, modificarea, controlul şi monitorizarea conturilor utilizator sunt operaţiuni foarte importante în cadrul general al asigurării securităţii sistemului RIC.

Scopul

Scopul Regulamentului pentru Administrarea Conturilor din Universitatea din Oradea este: stabilirea de reguli pentru crearea, utilizarea, monitorizarea, controlul şi ştergerea conturilor utilizator.

Audienta

Regulamentul pentru Administrarea Conturilor al Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor care au acces autorizat la sistemul de RIC din cadrul Universităţii din Oradea

Definiții

- *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.

REGULAMENT de administrare a conturilor de email

1. Toate conturile create trebuie să aibă asociată o cerere şi o aprobare corespunzătoare.
2. Toate conturile utilizator se vor crea în formatul Prenume.Nume, sau alternative.
3. Prin contractul de muncă, contractul de şcolarizare şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului RIC.
4. Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.
5. Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.
6. Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Regulamentul privind Parolele de Acces.
7. Conturile utilizator ale persoanelor plecate din Universitate pe timp îndelungat (mai mult de 180 de zile) vor fi dezactivate (conturile nu vor mai putea fi accesate), cu posibilitatea reactivării lor la solicitarea utilizatorului.

Administratorii de sisteme sau alt personal autorizat:

1. Sunt responsabili de ştergerea conturilor persoanelor (utilizatorilor) care nu mai lucrează în Universitatea din Oradea, sau care nu mai au relaţii cu Universitatea din Oradea.
2. Trebuie să aibă o documentaţie de modificare a conturilor utilizator pentru a se pune de acord în situaţii precum schimbări ale numelor de familie, modificări privind contul (numele contului) modificări ale drepturilor de utilizator.
3. Sunt subiectul verificării independente.
4. Trebuie să furnizeze o listă cu toţi utilizatorii (listă de conturi) pentru sistemele pe care le administrează, la cererea conducerii autorizate din Universitatea din Oradea.

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

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.
14. 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.
15. 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.
16. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu.
17. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.